

Decryption rules and Policy Example

This chapter builds on concepts discussed in this guide to provide a specific example of an SSL policy with decryption rules that follow our best practices and recommendations. You should be able to apply this example to your situation, adapting it to the needs of your organization.

In short:

- For trusted traffic (such as transferring a large compressed server backup), bypass inspection entirely, using prefiltering and flow offload.
- Put *first* any decryption rules that can be evaluated quickly, such as those that apply to specific IP addresses.
- Put *last* any decryption rules that require processing, **Decrypt - Resign**, and rules that block unsecure protocol versions and cipher suites.

- Decryption rule Examples, on page 1
- Run the Decryption Policy Wizard, on page 1
- First Manual Do Not Decrypt Rule: Specific Traffic, on page 7
- Next Manual Rule: Decrypt Specific Test Traffic, on page 9
- Last Manual Decryption rules: Block or Monitor Certificates and Protocol Versions, on page 10
- Associate the Decryption policy with an Access Control Policy and Advanced Settings, on page 16
- Traffic to Prefilter, on page 18
- Decryption rule Settings, on page 18

Decryption rule Examples

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

See one of the following sections for more information.

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 Create change management tickets and Policies and objects that support change management.

Procedure

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

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

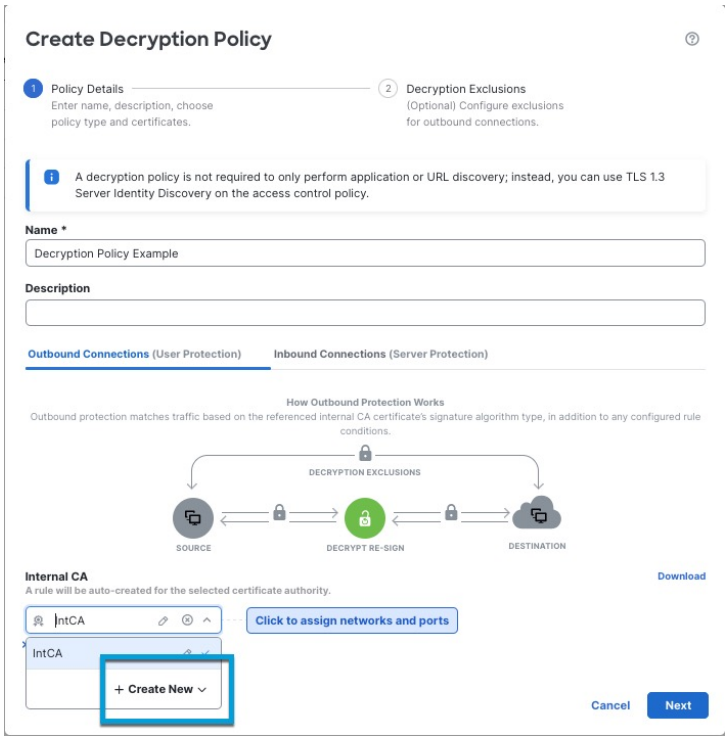
Step 3 Click **Create Decryption Policy**.

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.



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

- Upload an internal CA for outbound protection
- Generate an internal CA for outbound protection

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 Configure Decryption policy exclusions.

Configure Decryption policy exclusions

This task helps you create exclusions in your decryption policy to prevent decryption of traffic that should remain encrypted for compliance, security, or functional reasons.

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

Before you begin

You must upload an internal CA certificate for your managed device before you can create a decryption policy that protects outbound connections. You can do this in any of the following ways:

- Create an internal CA certificate object by going to **Objects** > **Object Management** > **PKI** > **Internal CAs** and referring to PKI objects.
- At the time you create this decryption policy.

Follow these steps to configure decryption policy exclusions:

Procedure

Step 1 Complete the tasks discussed in:

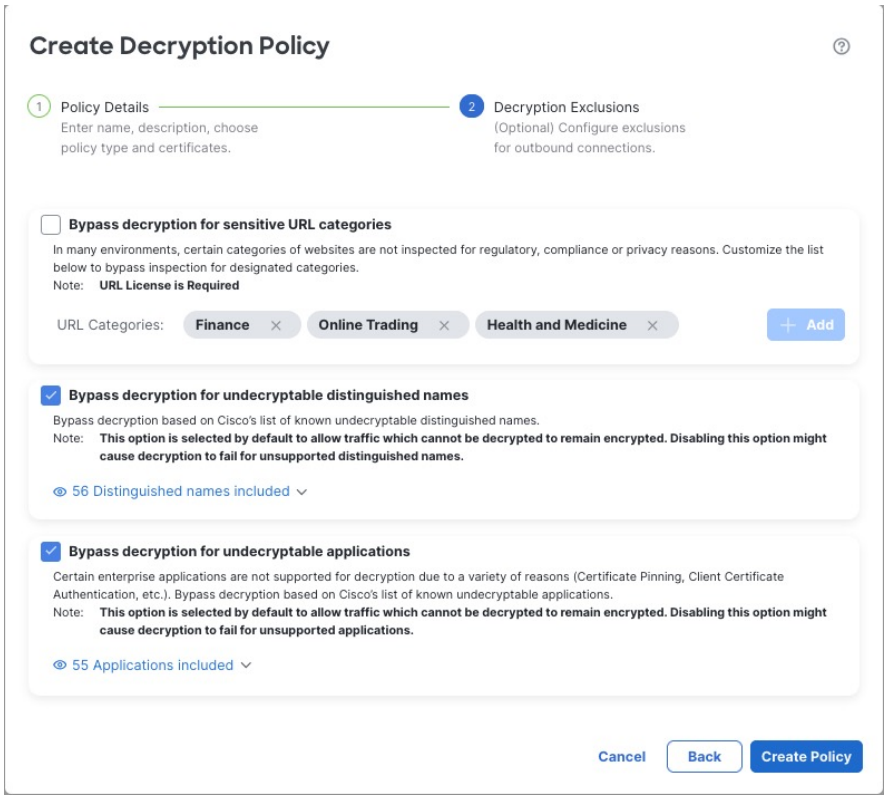
- Create a decryption policy with outbound connection protection
- For more information, see Create a decryption policy with inbound connection protection

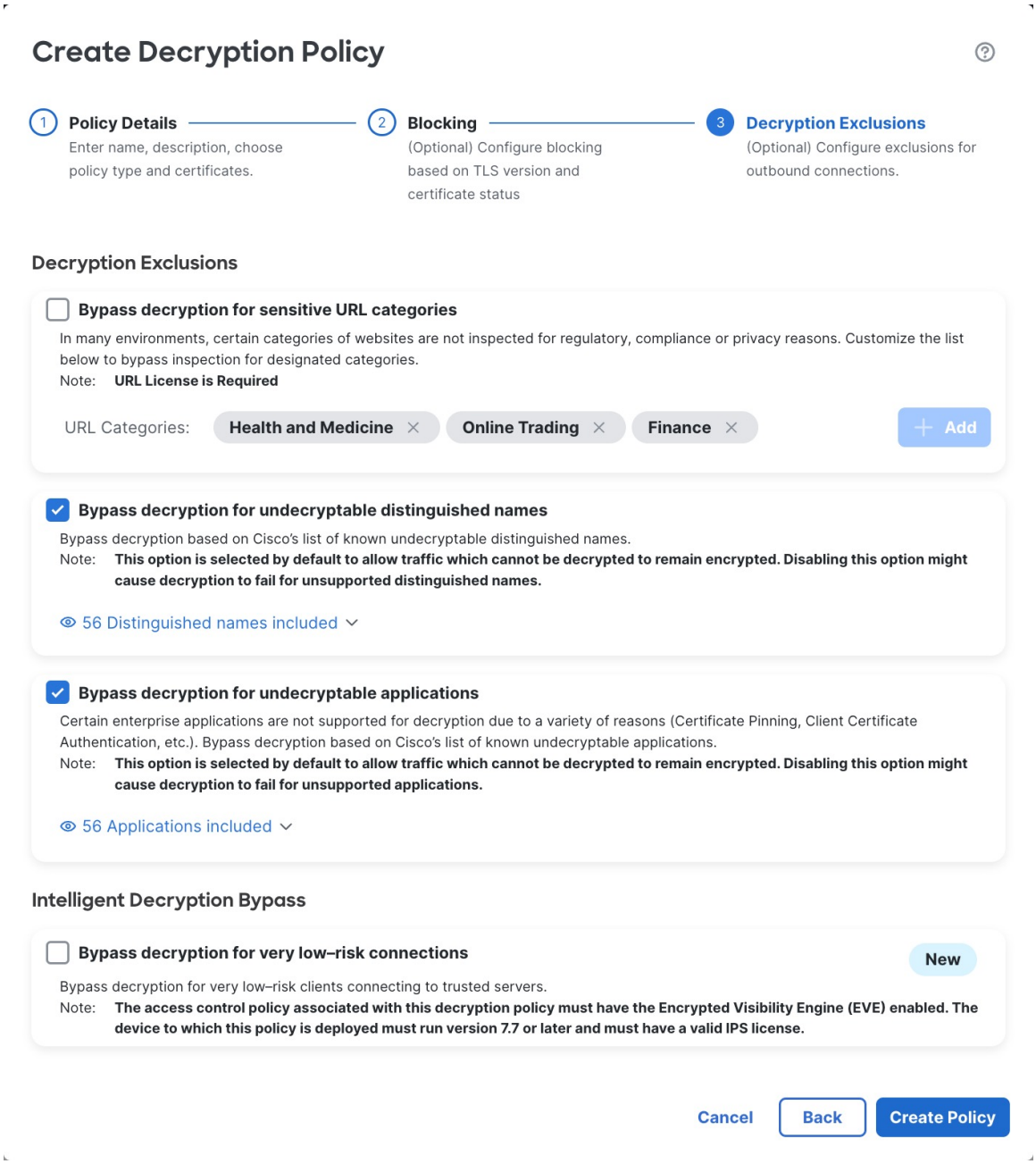
Step 2 Select the appropriate exclusion options based on your security requirements.

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 TLS/SSL certificate pinning guidelines. 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 TLS/SSL certificate pinning guidelines. 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.

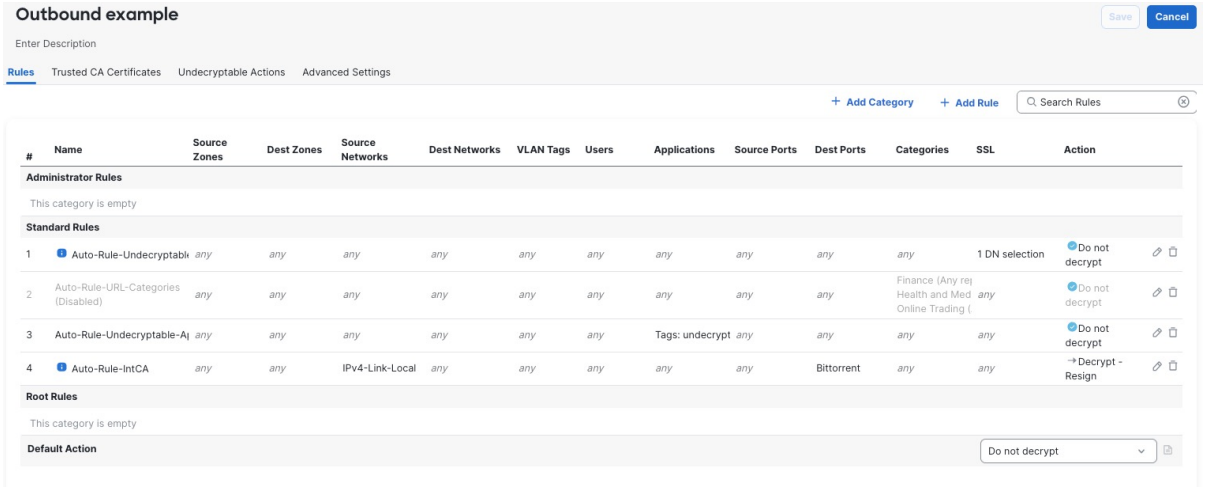
This figure shows default options.


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



Step 3 Click **Create Policy**.

This figure shows a sample outbound protection policy.



In the preceding example, the **Do Not Decrypt** rules corresponding to your choices for rule exclusions are automatically added before the **Decrypt - Resign** rule. The rule for sensitive URL categories is disabled because, by default, that exclusion is disabled. Had you selected the **Bypass decryption for sensitive URL categories** check box, the rule would have been enabled.

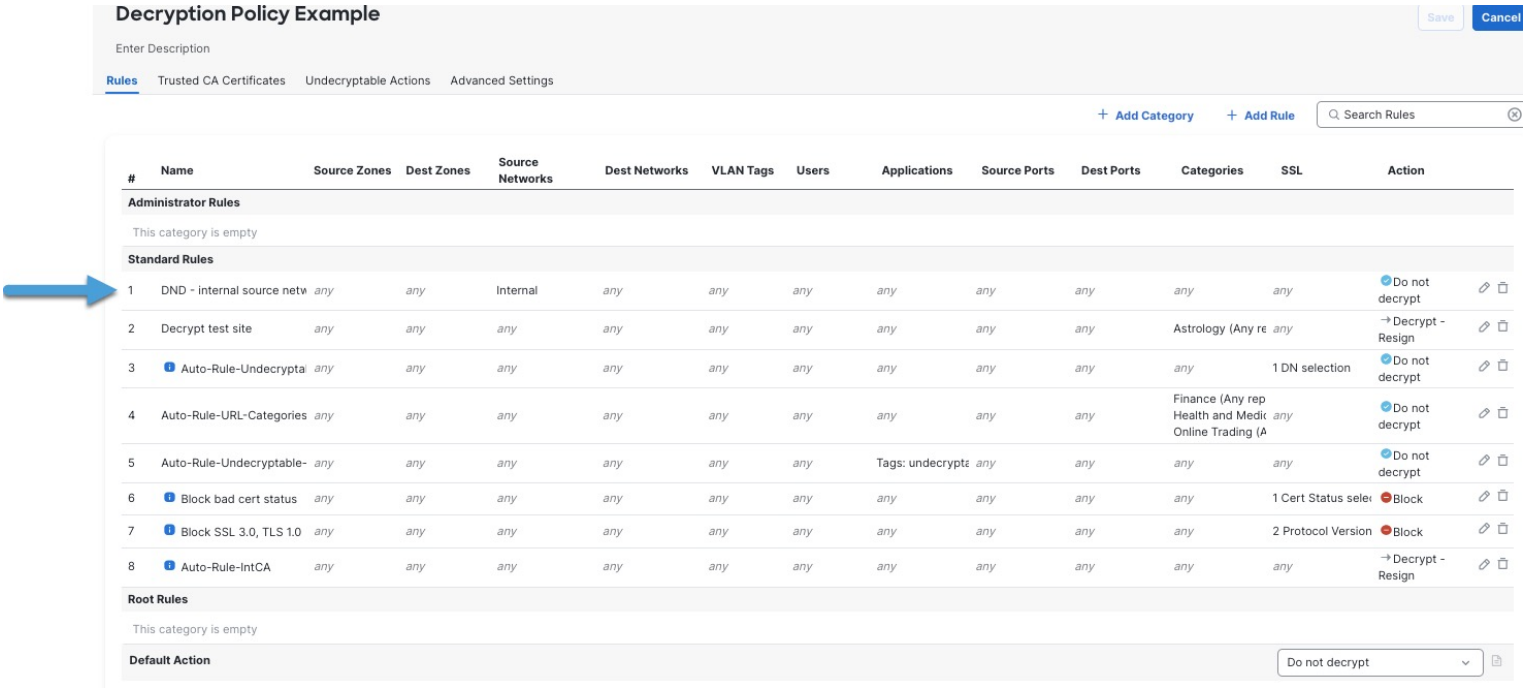
What to do next

- Add rule conditions: Decryption Rule conditions
- Add a default policy action: Decryption policy default actions
- Configure logging options for the default action as described in *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide* .
- Set advanced policy properties: Decryption policy advanced options.
- Associate the decryption policy with an access control policy as described in Associate prefilter, decryption, and identity policies with an access control.
- Deploy configuration changes; see Deploy configuration changes.

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.

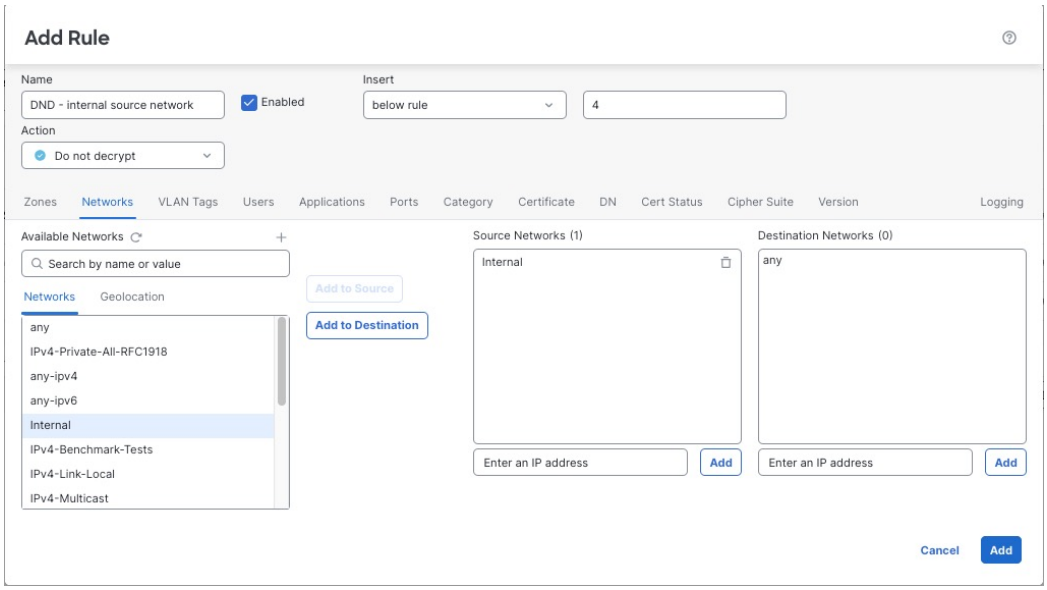
After you run the decryption policy wizard, edit the policy to add the following rule. Drag it to the top of the list of rules so it's evaluated first.



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.

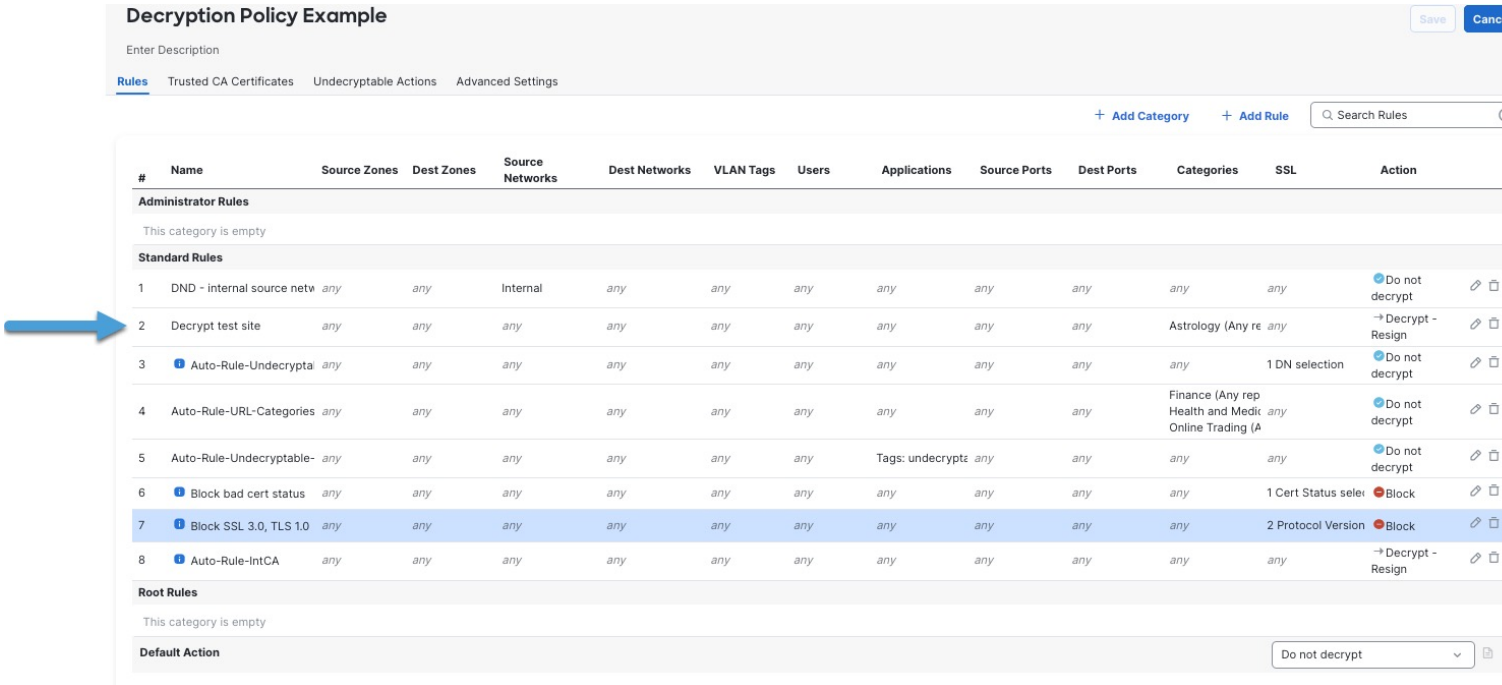
Rule detail:



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.

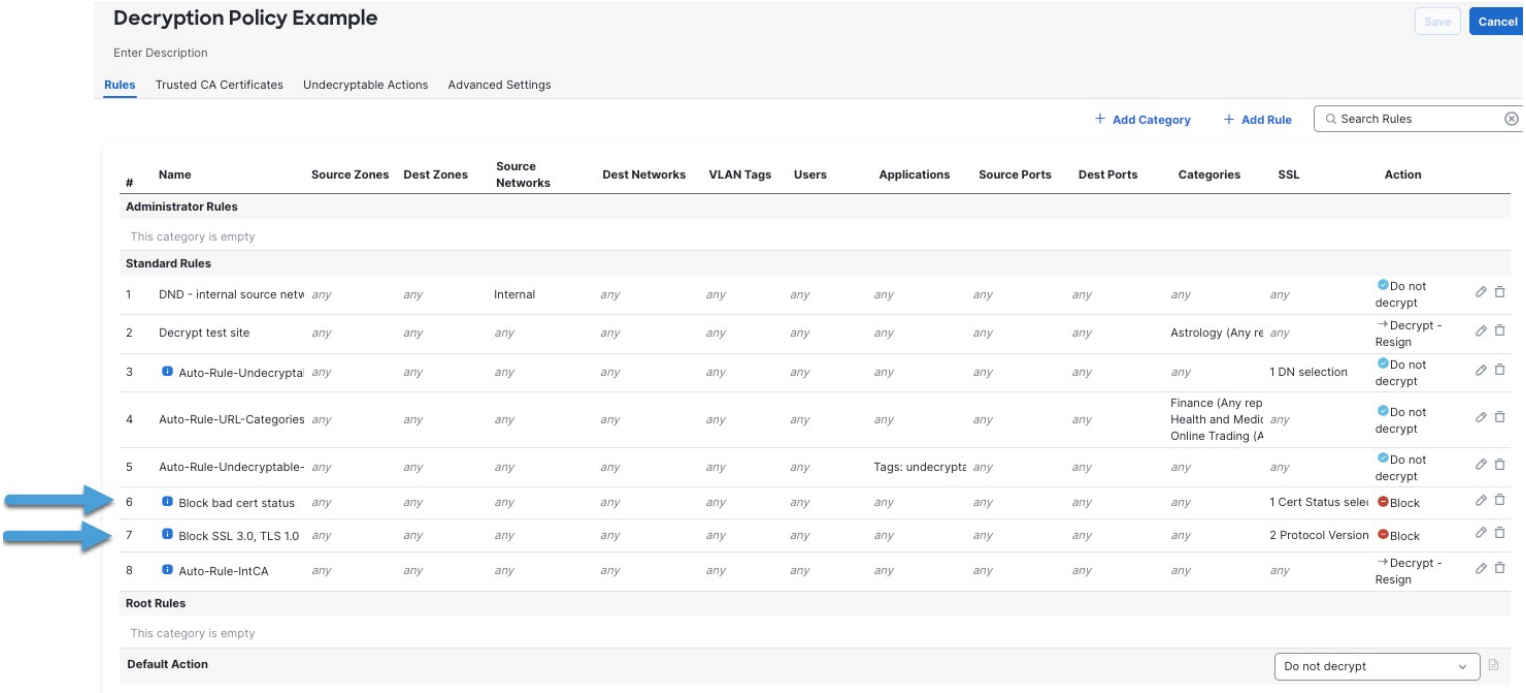


Rule detail:

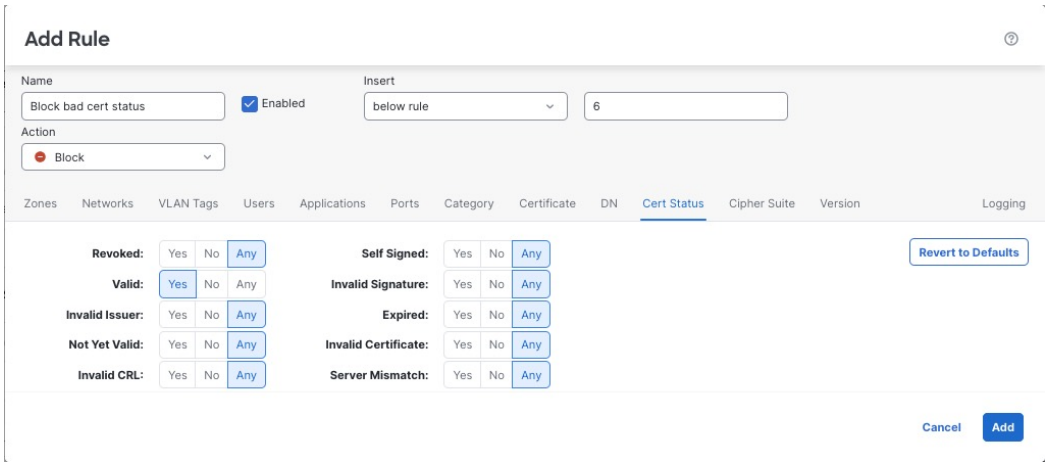
Last Manual Decryption rules: Block or Monitor Certificates and Protocol Versions

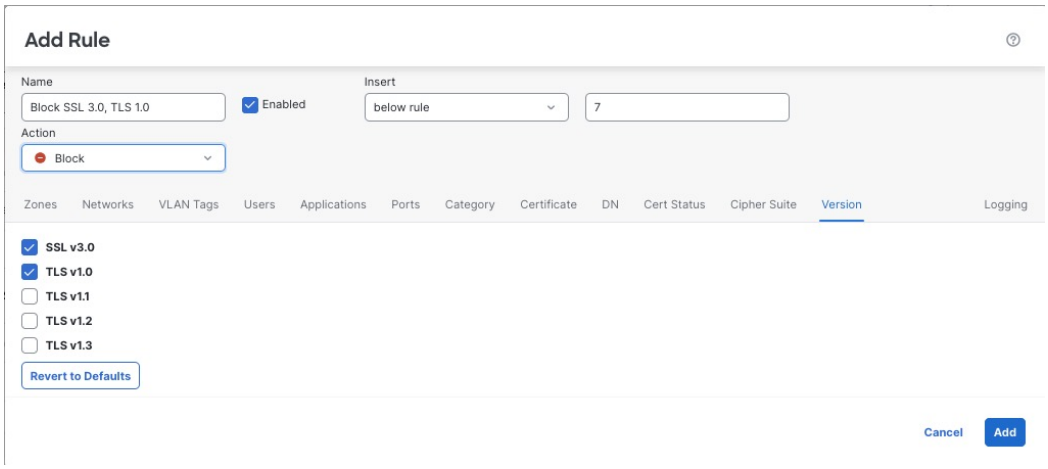
The last decryption rules, because they are the most specific and require the most processing, are rules that either monitor or block bad certificates and unsecure protocol versions.

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.



Rule details:





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

Procedure

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

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



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.



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.



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

Procedure

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

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

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

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

Step 5 Click **Add Rule**.

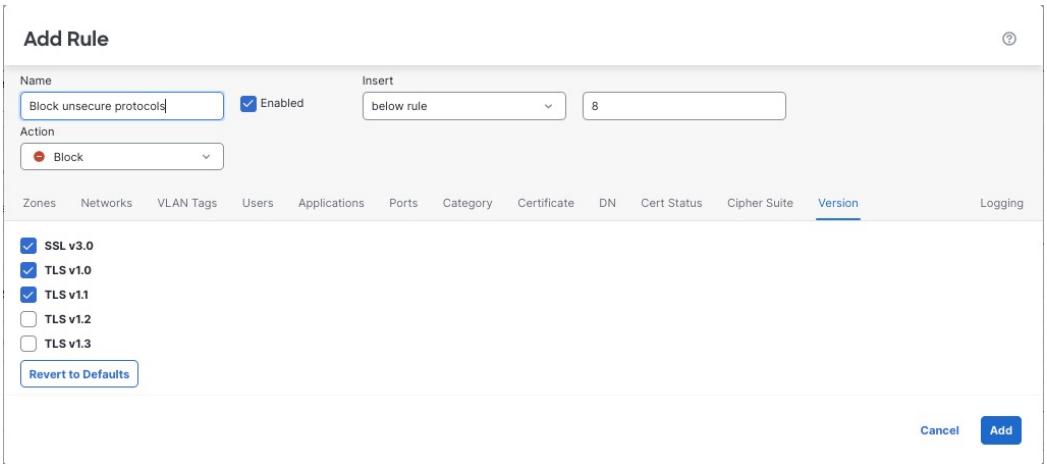
Step 6 In the Add Rule dialog box, in the **Name** field, enter a name for the rule.

Step 7 From the **Action** list, click **Block** or **Block with reset**.

Step 8 Click **Version** page.

Step 9 Check the check boxes for protocols that are no longer secure, such as **SSL v3.0**, **TLS 1.0**, and **TLS 1.1**. Clear the check boxes for any protocols that are still considered secure.

The following figure shows an example.



Step 10 Choose other rule conditions as needed.

Step 11 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; Conditions for distinguished name rules in decryption policies 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.

Procedure

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

Step 2 Click **Policies** > **Access Control heading** > **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 In the Add Rule dialog box, in the **Name** field, enter a name for the rule.

Step 7 From the **Action** list, click **Block** or **Block with reset**.

Step 8 Click **DN**.

Step 9 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 10 To select an object, click it. To select all objects, right-click and then **Select All**.

Step 11 Click **Add to Subject** or **Add to Issuer**.

Tip You can also drag and drop selected objects.

Step 12 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.

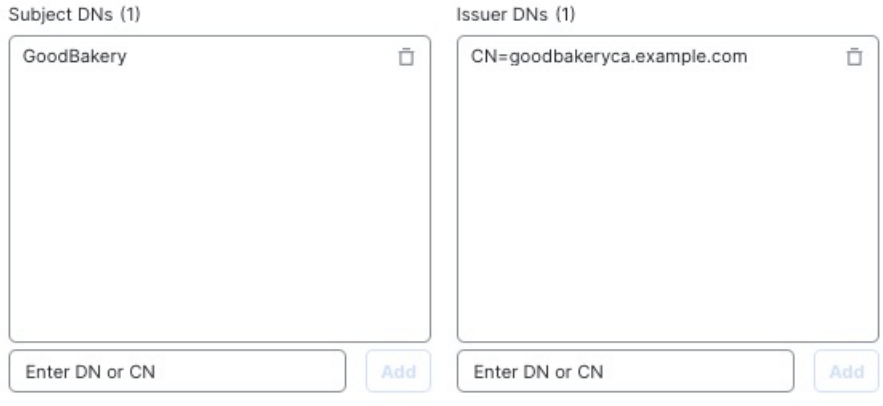
Step 13 Add or continue editing the rule.

Step 14 When you're done, to save changes to the rule, click **Add** at the bottom of the page.

Step 15 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.



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.

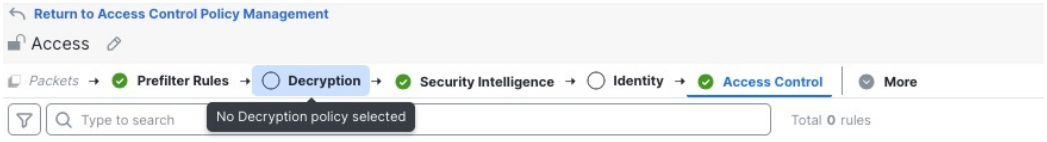
Procedure

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

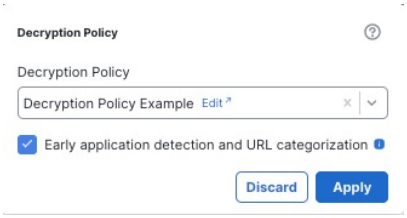
Step 2 Click **Policies** > **Access Control heading** > **Access Control**.

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.

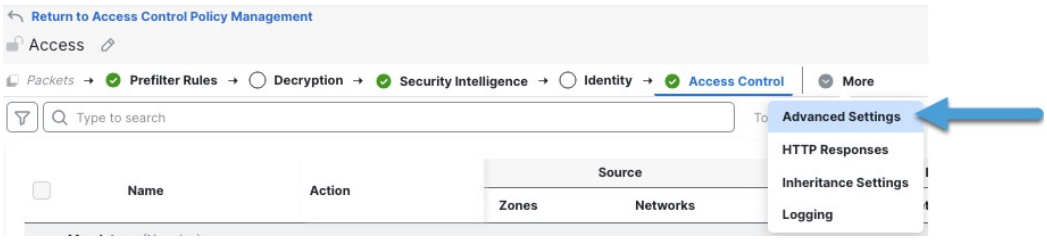


Step 5 From the list, click the name of your decryption policy and also check **Early application detection and URL categorization** as the following figure shows.



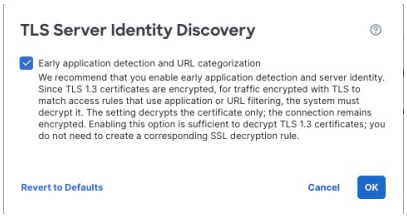
Step 6 Click **Apply**.

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



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

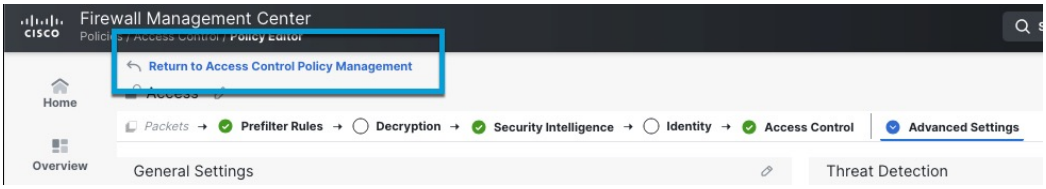
Step 9 Select the check box as the following figure shows.



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 policiesLogging 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 as described in *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide* .
- Set advanced policy properties: Decryption policy advanced options.
- Associate the decryption policy with an access control policy as described in Associate prefilter, decryption, and identity policies with an access control.
- Deploy configuration changes; see 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.)

Procedure

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

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

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

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

Step 5 Click the **Logging** tab.

Step 6 Click **Log at End of Connection**.

Step 7 Click **Save**.

Step 8 Click **Save** at the top of the page.