Deploy TLS/SSL Rules With Examples 7.2

First Published: 2022-02-22

Last Modified: 2022-11-21

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

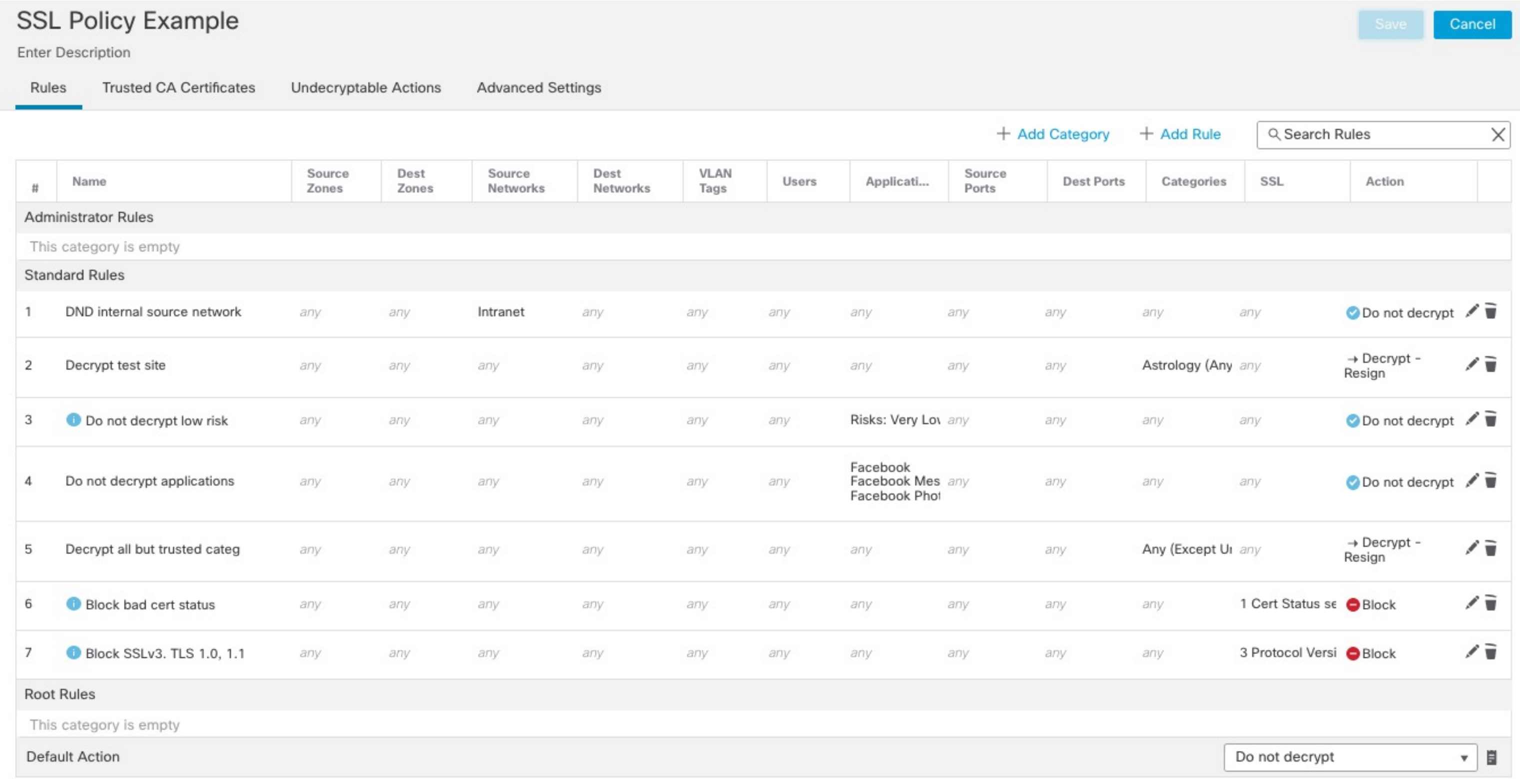
CHAPTER 1

TLS/SSL Rules Best Practices

TLS/SSL Rules Best Practices

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

Following is the SSL policy we'll discuss in this chapter.



SSL Policy Example

Enter Description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	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	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lo\	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ui	any	→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
Root Rules													
This category is empty													
Default Action													Do not decrypt

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 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.

Do Not Decrypt Best Practices

Log traffic

We recommend *against* creating **Do Not Decrypt** rules that do not log anything because these rules still take processing time on the managed device. If you set up any type of TLS/SSL rules, *enable logging* so you can see what traffic is being matched.

Guidelines for undecryptable traffic

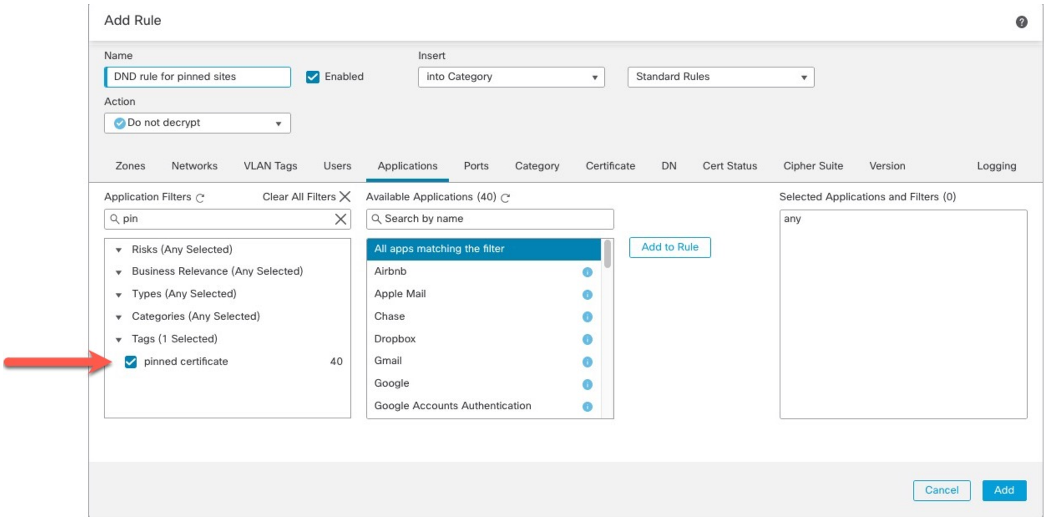
We can determine that certain traffic is not decryptable either because the website itself is not decryptable or because the website uses SSL pinning, which effectively prevents users from accessing a decrypted site without errors in their browser.

We maintain the list of these sites as follows:

- A Distinguised Name (DN) group named **Cisco-Undecryptable-Sites**
- The **pinned certificate** 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 TLS/SSL rules.

An example of setting up a **pinned certificate** application filter follows.



Add Rule

Name: DND rule for pinned sites ☑ Enabled

Insert: into Category — Standard Rules

Action: Do not decrypt

Application Filters: pin

- Risks (Any Selected)
- Business Relevance (Any Selected)
- Types (Any Selected)
- Categories (Any Selected)
- Tags (1 Selected)
  - ☑ pinned certificate 40

Available Applications (40):

- All apps matching the filter
- Airbnb
- Apple Mail
- Chase
- Dropbox
- Gmail
- Google
- Google Accounts Authentication

Selected Applications and Filters (0): any

Decrypt - Resign and Decrypt - Known Key Best Practices

This topic discusses best practices for **Decrypt - Resign** and **Decrypt - Known Key** TLS/SSL rule.

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 TLS/SSL 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. You have the following options:

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

For more information about certificate pinning, see the section on 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 a destination network to these rules (**Networks** rule condition). That way the traffic goes directly to the network on which the server is located, thereby reducing traffic on the network.

TLS/SSL 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).

TLS/SSL Rules to Put Last

Rules with the following rule conditions should be last because those rules require traffic to be examined for the longest amont of time by the system:

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

CHAPTER 2

Recommended Policy and Rule Settings

Recommended Policy and Rule Settings

We recommend the following policy settings:

- SSL 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 in the policy's advanced settings.
- TLS/SSL rule: 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 SSL policy with an access control policy. (If you fail to do this, your SSL policy and rules have no effect.)
  - Set the default policy action to **Intrusion Prevention: Balanced Security and Connectivity**.
  - Enable logging.

Related Topics

SSL Policy Settings, on page 6
TLS/SSL Rule Settings, on page 20
Access Control Policy Settings, on page 7

SSL Policy Settings

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

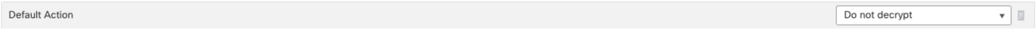
- Default action **Do Not Decrypt**.
- Enable logging.
- Set **Undecryptable Actions** to **Block** for both **SSL v2 Session** and **Compressed Session**.
- Enable TLS 1.3 decryption in the policy's advanced settings.

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

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

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

Step 4 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 5 At the end of the row, click **Logging** (🗎).

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

Step 7 Click **OK**.

Step 8 Click **Save**.

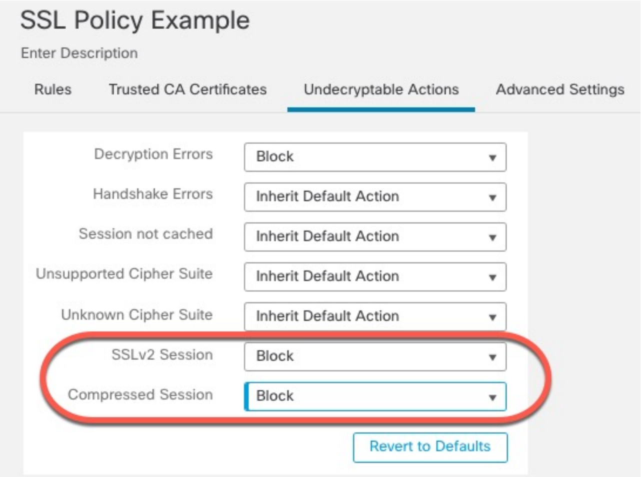
Step 9 Click the **Undecryptable Actions** tab.

Step 10 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 the section on 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.



SSL Policy Example

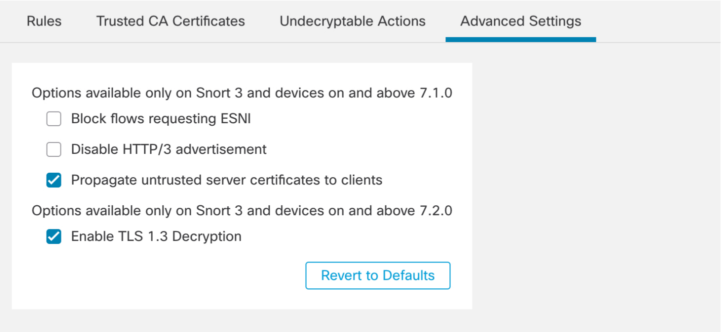
Enter Description

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 11 Click the **Advanced Settings** tab page.

Step 12 Select the **Enable TLS 1.3 Decryption** check box.

Following is an example.



Options available only on Snort 3 and devices on and above 7.1.0

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

Options available only on Snort 3 and devices on and above 7.2.0

- ☑ Enable TLS 1.3 Decryption

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

What to do next

Configure TLS/SSL rules and set each one as discussed in TLS/SSL Rule Settings, on page 20.

Access Control Policy Settings

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

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

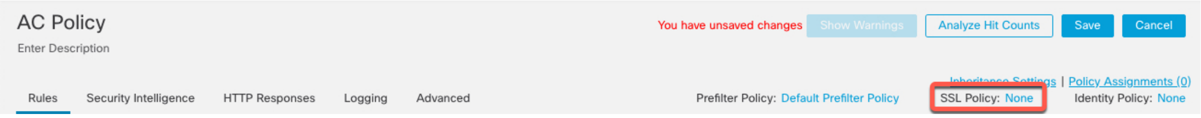
Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

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

Step 3 Click **Edit** () next to your access control policy.

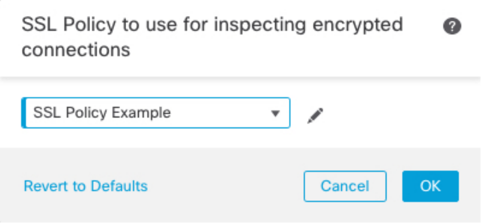
Step 4 (If your SSL policy isn't set up yet, you can do this later.)

a) Click the word **None** next to **SSL Policy** at the top of the page as the following figure shows.



Prefilter Policy: Default Prefilter Policy
SSL Policy: None
Identity Policy: None

b) From the list, click the name of your SSL policy. The following figure shows an example.

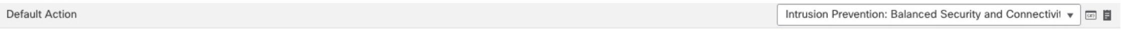

SSL Policy to use for inspecting encrypted connections

SSL Policy Example

c) Click **OK**.

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

Step 5 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 6 Click **Logging** ().

Step 7 Select the **Log at End of Connection** check box and click **OK**.

Step 8 Click **Save**.

What to do next

See TLS/SSL Rule Examples, on page 9.

CHAPTER 3

TLS/SSL Rule Examples

TLS/SSL Rule Examples

This chapter provides an example of TLS/SSL rule that illustrate our best practices.

Traffic to Prefilter

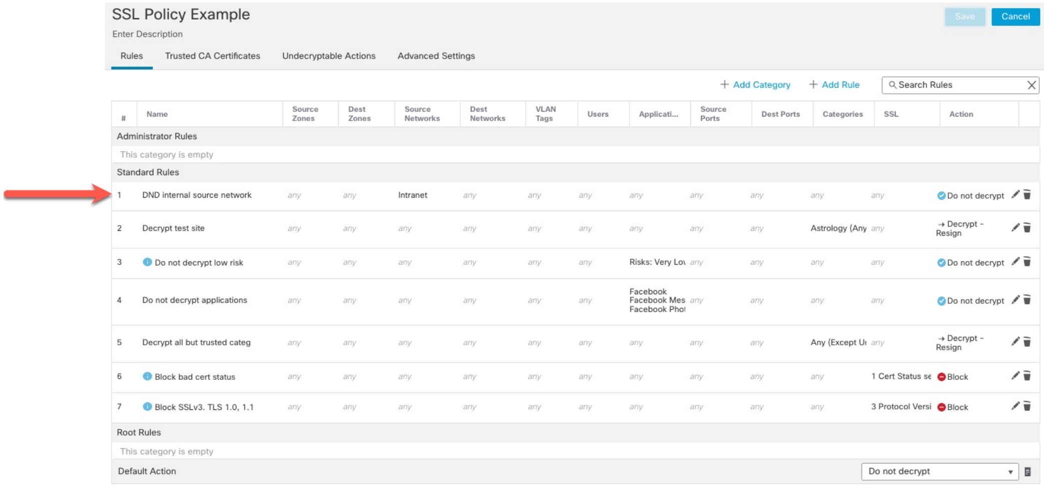
Prefiltering is the first phase of access control, before the system performs more resource-intensive evaluation. Prefiltering is simple, fast, and early compared to subsequent evaluation, which uses inner headers and has more robust inspection capabilities.

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

First TLS/SSL Rule: Do Not Decrypt Specific Traffic

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



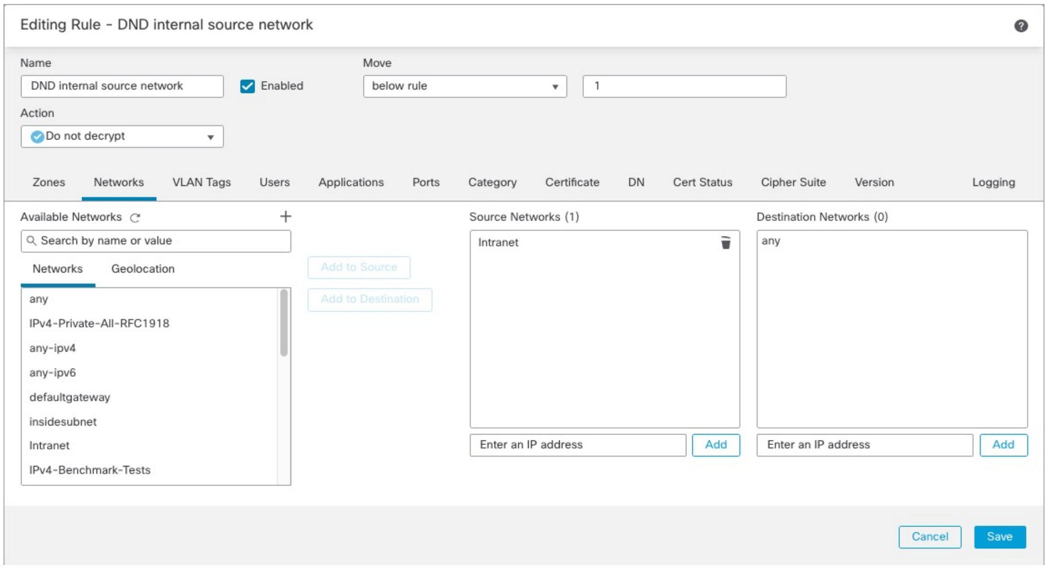
SSL Policy Example

Enter Description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	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	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ui	any	→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
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.



Editing Rule - DND internal source network

Name: DND internal source network ☑ Enabled

Move: below rule 1

Action: Do not decrypt

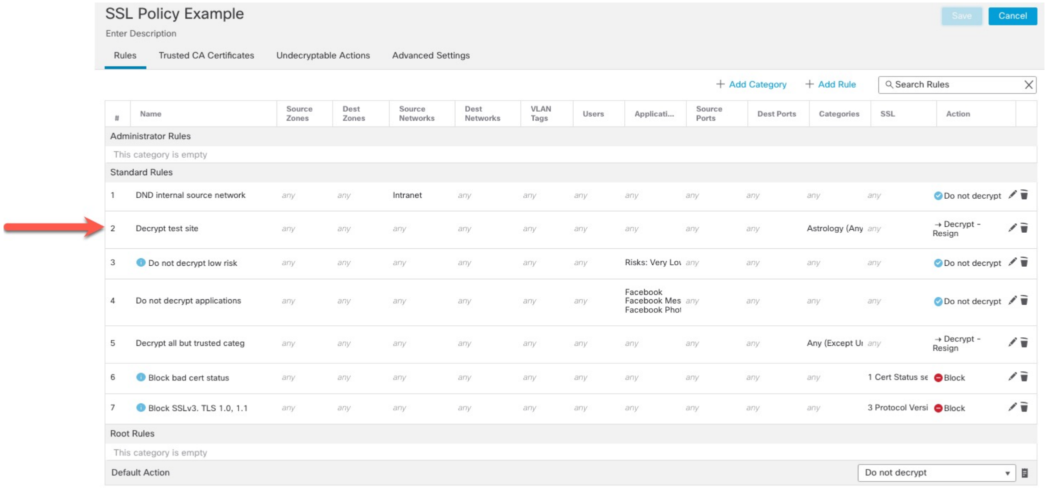
Available Networks:
any
IPv4-Private-All-RFC1918
any-ipv4
any-ipv6
defaultgateway
insidesubnet
Intranet
IPv4-Benchmark-Tests

Source Networks (1): Intranet

Destination Networks (0): any

Next TLS/SSL Rules: 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.

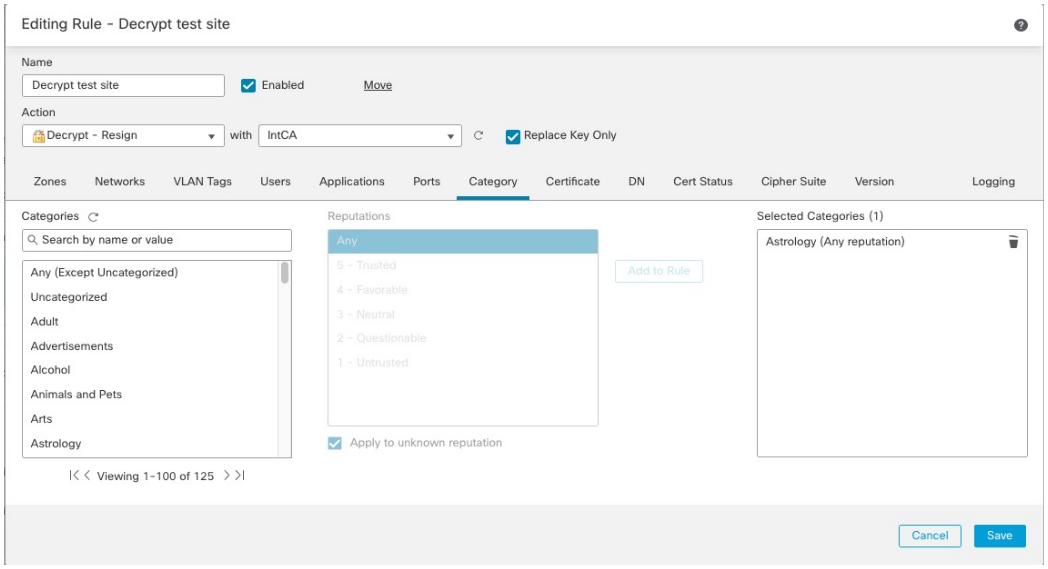


SSL Policy Example

Enter Description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	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	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ur	any	→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
Root Rules													
This category is empty													
Default Action													Do not decrypt

Rule detail:



Editing Rule - Decrypt test site

Name: Decrypt test site ☑ Enabled Move

Action: Decrypt - Resign with IntCA ☑ Replace Key Only

Categories

Reputations

☑ Apply to unknown reputation

Selected Categories (1)

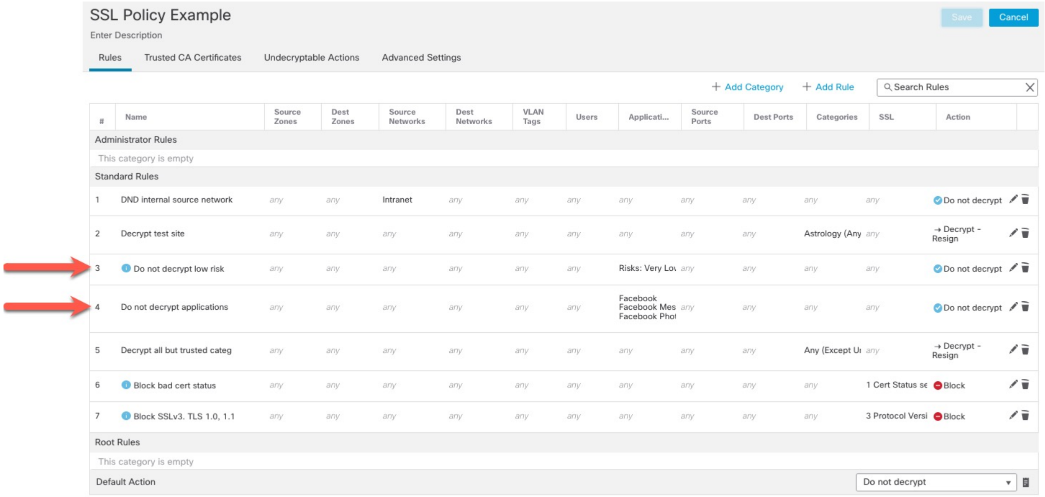
Astrology (Any reputation)

Do Not Decrypt Low-Risk Categories, Reputations, or Applications

Evaluate the traffic on your network to determine which would match low-risk categories, reputations, or applications, and add those rules with a **Do Not Decrypt** action. Put these rules *after* other more specific **Do Not Decrypt** rules because the system needs more time to process the traffic.

Following is the example.

Do Not Decrypt Low-Risk Categories, Reputations, or Applications

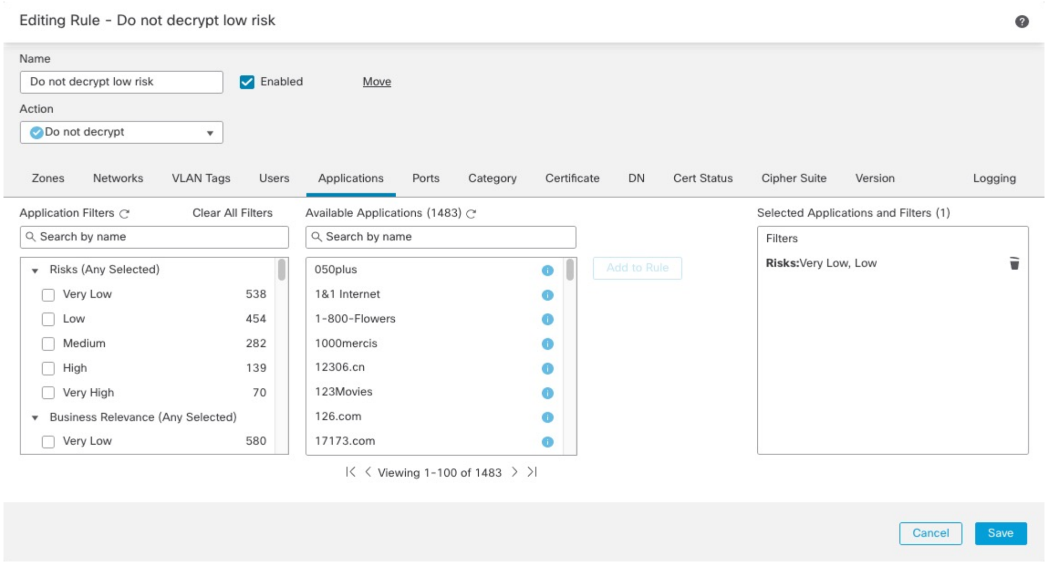


SSL Policy Example

Enter Description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	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	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	✓ Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	✓ Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ui	any	→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
Root Rules													
This category is empty													
Default Action													Do not decrypt

Rule details:



Editing Rule - Do not decrypt low risk

Name: Do not decrypt low risk ☑ Enabled Move

Action: ✓ Do not decrypt

Application Filters — Clear All Filters

Search by name

- Risks (Any Selected)

□ Very Low	538
□ Low	454
□ Medium	282
□ High	139
□ Very High	70

- Business Relevance (Any Selected)

□ Very Low	580

Available Applications (1483)

Search by name

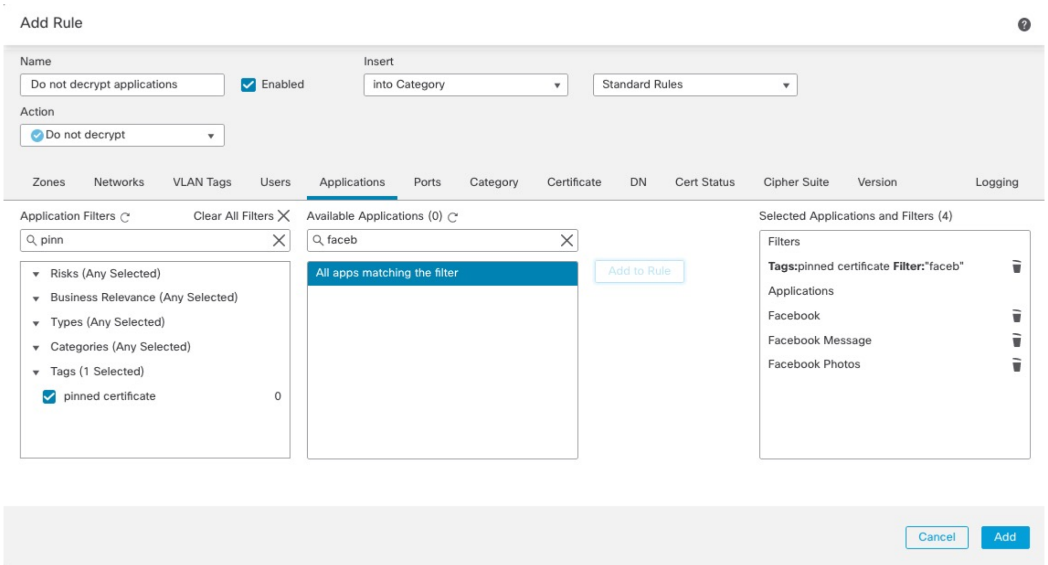
050plus
1&1 Internet
1-800-Flowers
1000mercis
12306.cn
123Movies
126.com
17173.com

Viewing 1-100 of 1483

Selected Applications and Filters (1)

Filters

Risks: Very Low, Low



Name: Do not decrypt applications

☑ Enabled

Insert: into Category | Standard Rules

Action: Do not decrypt

Application Filters

pinn

- Risks (Any Selected)
- Business Relevance (Any Selected)
- Types (Any Selected)
- Categories (Any Selected)
- Tags (1 Selected)
  - ☑ pinned certificate 0

Available Applications (0)

faceb

All apps matching the filter

Selected Applications and Filters (4)

Filters

Tags:pinned certificate **Filter:**"faceb"

Applications

Facebook

Facebook Message

Facebook Photos

Create a Decrypt - Resign Rule for Categories

This topic shows an example of creating a TLS/SSL rule with a **Decrypt - Resign** action for all but uncategorized sites. The rule uses the optional **Replace Key Only** option, which we always recommend with a **Decrypt-Resign** rule action.

Replace Key Only causes the user to see a security warning in the web browser when they browse to a site that uses a self-signed certificate, making the user aware that they are communicating with an unsecure site.

By putting this rule near the bottom, you get the best of both worlds: you can decrypt and optionally inspect traffic while not affecting performance as much as if you had put the rule earlier in the policy.

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

Step 2 If you haven't already done so, upload an internal certificate authority (CA) to the Secure Firewall Management Center (**Objects** > **Object Management**, then **PKI** > **Internal CAs**).

Step 3 Click **Policies** > **Access Control** > **SSL**.

Step 4 Click **Edit** (✎) next to your SSL policy.

Step 5 Click **Add Rule**.

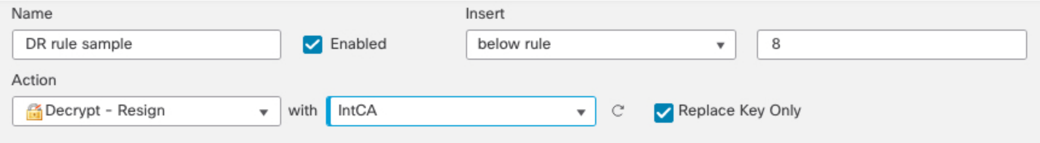
Step 6 In the **Name** field, enter a name to identify the rule.

Step 7 From the **Action** list, click **Decrypt - Resign**.

Step 8 From the **with** list, click the name of your internal CA.

Step 9 Check the **Replace Key Only** box.

The following figure shows an example.



Name: DR rule sample

☑ Enabled

Insert: below rule | 8

Action: Decrypt - Resign with IntCA

☑ Replace Key Only

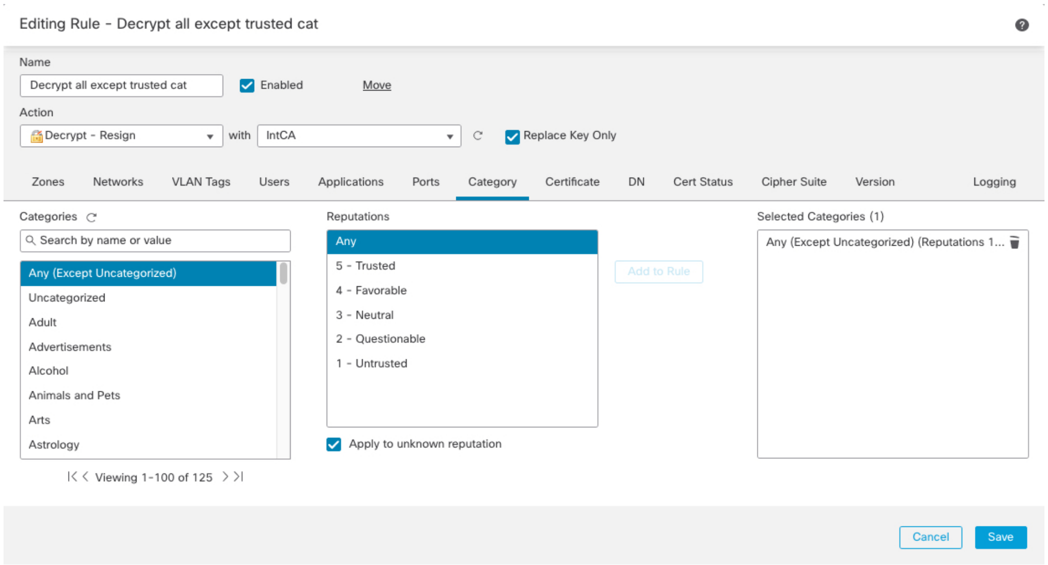
Step 10 Click the **Category** tab page.

Step 11 From the top of the **Categories** list, click **Any (Except Uncategorized)**.

Step 12 From the **Reputations** list, click **Any**.

Step 13 Click **Add to Rule**.

The following figure shows an example.



Editing Rule - Decrypt all except trusted cat

Name: Decrypt all except trusted cat ☑ Enabled Move

Action: Decrypt - Resign with IntCA ☑ Replace Key Only

Categories: Search by name or value
- Any (Except Uncategorized)
- Uncategorized
- Adult
- Advertisements
- Alcohol
- Animals and Pets
- Arts
- Astrology

Viewing 1-100 of 125

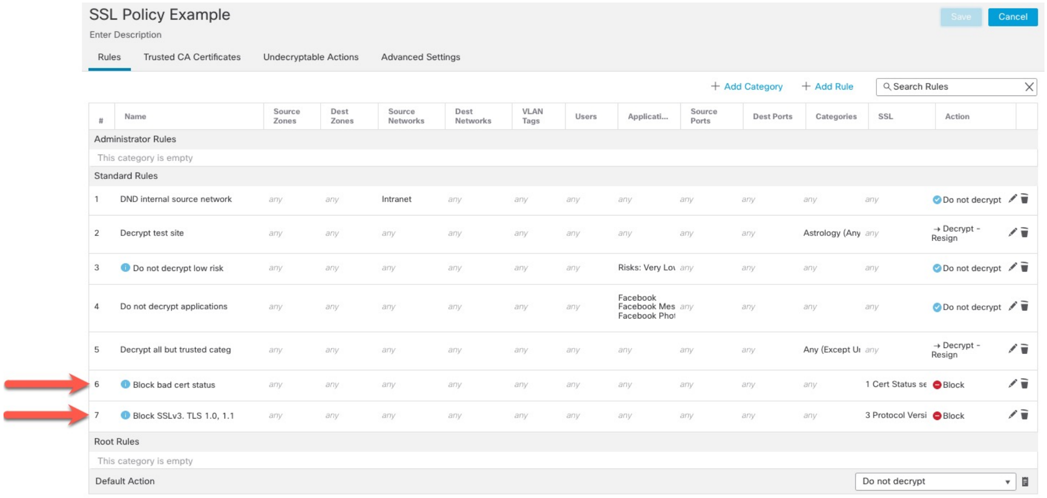
Reputations:
- Any
- 5 - Trusted
- 4 - Favorable
- 3 - Neutral
- 2 - Questionable
- 1 - Untrusted

☑ Apply to unknown reputation

Selected Categories (1): Any (Except Uncategorized) (Reputations 1...

Last TLS/SSL Rules: Block or Monitor Certificates and Protocol Versions

The last TLS/SSL 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.

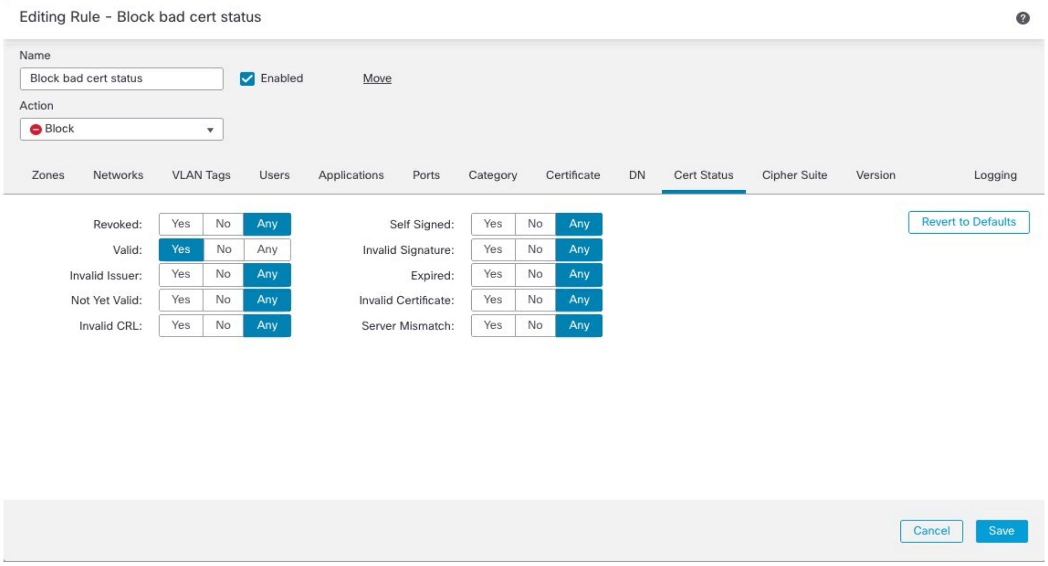


SSL Policy Example

Enter Description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	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	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lo\	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ui	any	→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
Root Rules													
This category is empty													
Default Action													Do not decrypt

Rule details:

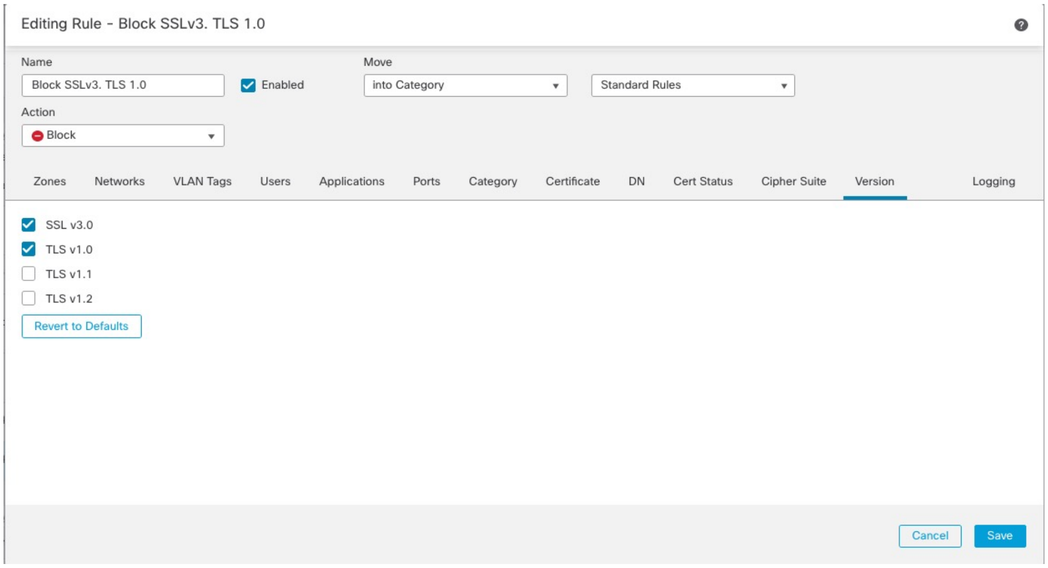


Editing Rule - Block bad cert status

Name: Block bad cert status
☑ Enabled
Action: Block

Cert Status:

	Yes	No	Any		Yes	No	Any
Revoked:			●	Self Signed:			●
Valid:	●			Invalid Signature:			●
Invalid Issuer:			●	Expired:			●
Not Yet Valid:			●	Invalid Certificate:			●
Invalid CRL:			●	Server Mismatch:			●



Editing Rule - Block SSLv3. TLS 1.0

Name: Block SSLv3. TLS 1.0
☑ Enabled
Move: into Category — Standard Rules
Action: Block

Version:

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

Example: TLS/SSL Rule to Monitor or Block Certificate Status

The last TLS/SSL 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.

Note 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** > **SSL**.

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

Step 4 Click **Edit** (✎) next to a TLS/SSL 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.

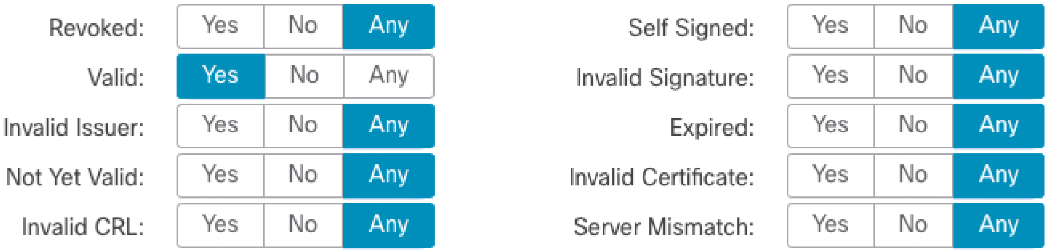
Step 10 To save changes to the rule, at the bottom of the page, click **Save**.

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

Example

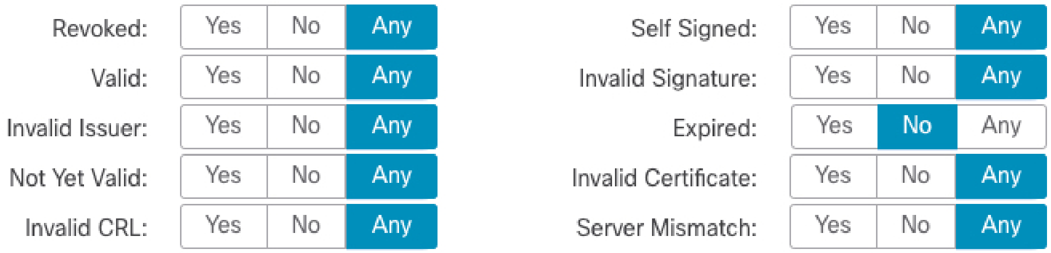
The organization trusts the Verified Authority certificate authority. The organization does not trust the Spammer Authority certificate authority. The system administrator uploads the Verified Authority certificate and an intermediate CA certificate issued by Verified Authority to the system. Because 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]

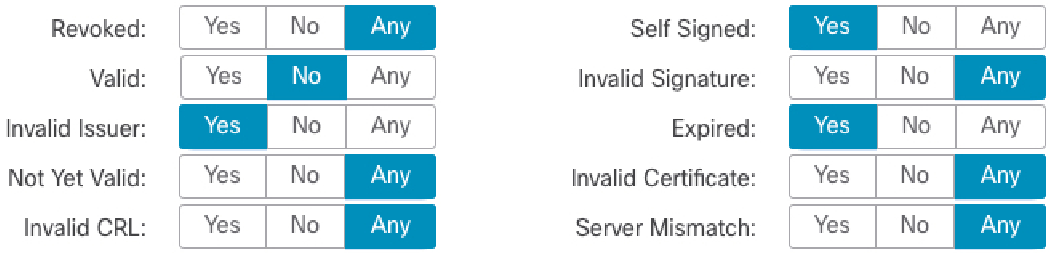
The following figure shows a certificate status rule condition checking for the absence of a status. In this case, because of the configuration, it matches against traffic encrypted with a certificate that has not expired and monitors that traffic.



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]

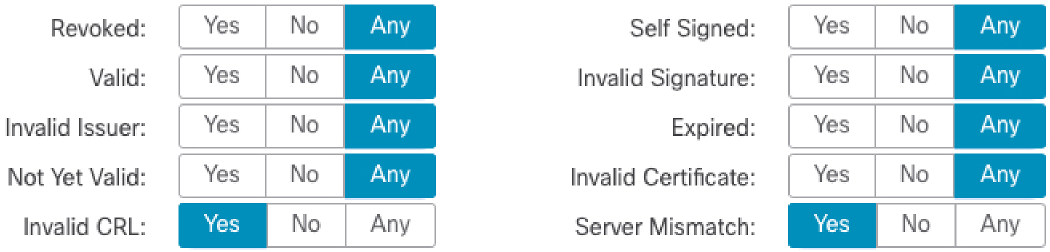
In the following example, traffic would match this rule condition if the incoming traffic is using a certificate that has an invalid issuer, is self-signed, expired, and it is an invalid certificate.



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

Note 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** > **SSL**.

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

Step 4 Click **Edit** (✎) next to a TLS/SSL rule.

Step 5 Click **Add Rule**.

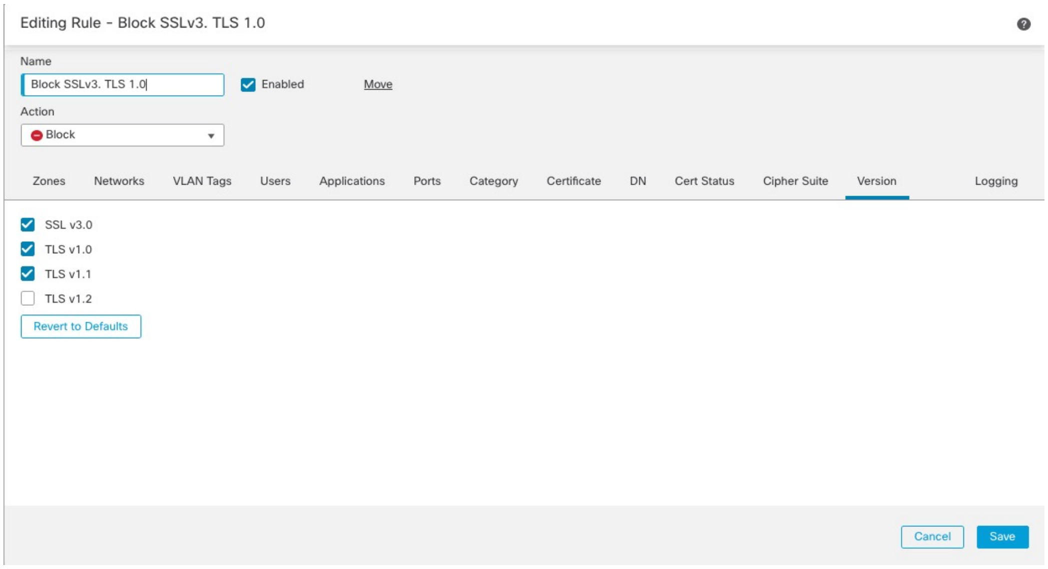
Step 6 In the Add Rule dialog box, in the **Name** field, enter a name for the rule.

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.



Editing Rule - Block SSLv3. TLS 1.0

Name: Block SSLv3. TLS 1.0

☑ Enabled

Action: Block

☑ SSL v3.0
☑ TLS v1.0
☑ TLS v1.1
□ TLS v1.2

Step 10 Choose other rule conditions as needed.

Step 11 Click **Save**.

Optional Example: TLS/SSL 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 Distinguished Name. 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; the section on 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 Log in to the Secure Firewall Management Center if you haven't already done so.

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

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

Step 4 Click **Edit** (✎) next to a TLS/SSL 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 **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.

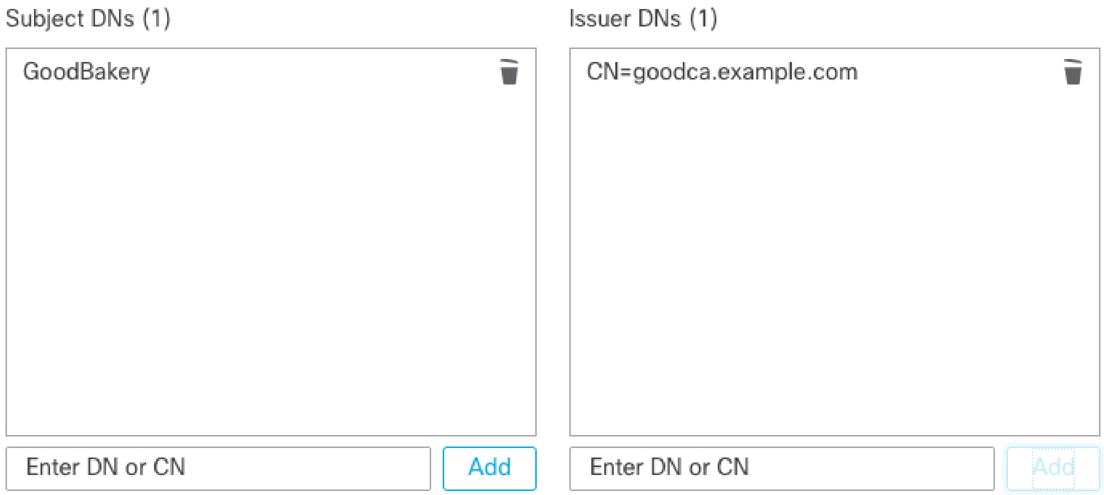
Step 13 Add or continue editing the rule.

Step 14 When you're done, to save changes to the rule, click **Save** 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.



Subject DNs (1)

GoodBakery

Issuer DNs (1)

CN=goodca.example.com

TLS/SSL Rule Settings

How to configure recommended best practice settings for your TLS/SSL rules.

TLS/SSL rule: 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 Log in to the Secure Firewall Management Center if you haven't already done so.

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

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

Step 4 Click **Edit** (✎) next to a TLS/SSL 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.