

# **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 Rules Best Practices, on page 1
- Decryption Policy Walkthrough, on page 4

# **Decryption Rules Best Practices**

This chapter provides an example SSL policy with decryption 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

Rule	s Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	etungs									
									+	Add Category	+ Add Rule	Q Search R	ules	
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
dmi	nistrator Rules													
This	category is empty													
Stand	lard Rules													
Î.	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	OD not decrypt	1
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign	
3	O not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	Oo not decrypt	/
ı	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 U	any	→ Decrypt - Resign	
5	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block	
	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	/
loot	Rules													
This	category is empty													
Defa	ult 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.

#### **Related Topics**

Large Flow Offloads Prefiltering vs Access Control Best Practices for Fastpath Prefiltering

### **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 decryption 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.

For more information about certificate pinning, see About TLS/SSL Pinning.

We maintain the list of these sites as follows:

- A Distinguished 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 decryption rules.

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

Name		Insert					
DND rule for pinned sites	Enabled	into Category	¥	Standard Rules	-		
Action							
📀 Do not decrypt 🔹 👻							
Zones Networks VLAN Tags	Users	Applications Ports Ca	ategory Certificat	e DN Cert Status	Cipher Suite	Version	I
Application Filters C Clear All	I Filters 🗙	Available Applications (40) C			Selected Applic	ations and Filters (0)	
Q pin	×	Q Search by name			any		
<ul> <li>Risks (Any Selected)</li> </ul>		All apps matching the filter		Add to Rule			
<ul> <li>Business Relevance (Any Selected)</li> </ul>		Airbnb	0				
▼ Types (Any Selected)		Apple Mail	0				
<ul> <li>Categories (Any Selected)</li> </ul>		Chase	0				
▼ Tags (1 Selected)		Dropbox	0				
pinned certificate	40	Gmail	0				
		Google	0				
		Google Accounts Authenticatio	on 🕜				

### **Decrypt - Resign and Decrypt - Known Key Best Practices**

This topic discusses best practices for Decrypt - Resign and Decrypt - Known Key decryption 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 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. 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 About TLS/SSL Pinning.

#### **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.

### **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 Last**

Rules with the following rule conditions should be last 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

# **Decryption Policy Walkthrough**

This chapter provides a step-by-step discussion and walkthrough of how to create a decryption policy using rules that employ our best practices. You'll see a preview of the decryption policy followed by a synopsis of the best practices and finally a discussion of the rules in the policy.

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

#### SSL Policy Example

Enter Description

									+ /	Add Category	+ Add Rule	Q Search R	ules	>
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
dminis	strator Rules													
his ca	ategory is empty													
anda	rd Rules													
D	ND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Op not decrypt	1
D	ecrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign	1
•	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	OD not decrypt	1
D	o not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot		any	any	any	🕑 Do not decrypt	/1
D	ecrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ur	any	→ Decrypt - Resign	1
•	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block	1
•	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	1
oot Ru	lles													

See one of the following sections for more information.

#### **Related Topics**

Recommended Policy and Rule Settings, on page 5 Traffic to Prefilter, on page 9 First Decryption Rule: Do Not Decrypt Specific Traffic, on page 9 Next Decryption Rules: Decrypt Specific Test Traffic, on page 10 Create a Decrypt - Resign Rule for Categories, on page 12 Do Not Decrypt Low-Risk Categories, Reputations, or Applications, on page 11 Last Decryption Rules: Block or Monitor Certificates and Protocol Versions, on page 14

## **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 in the policy's advanced settings.
- decryption 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 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.

Decryption Policy Settings, on page 6 Decryption Rule Settings, on page 20 Access Control Policy Settings, on page 7

#### **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 in the policy's advanced settings.

#### Procedure

Step 1 Step 2	Log in to the Secure Firewall Management Center if you be Click <b>Policies</b> > <b>Access Control</b> > <b>Decryption</b> .	naven't already done so.
Step 3 Step 4	Click <b>Edit</b> ( <i>I</i> ) next to your decryption policy. From the <b>Default Action</b> list at the bottom of the page, cli The following figure shows an example.	ick <b>Do Not Decrypt</b> .
	Default Action	Do not decrypt
Step 5	At the end of the row, click <b>Logging</b> (	
Step 6	Select the Log at End of Connection check box.	
Step 7	Click <b>OK</b> .	
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 compress	sed TLS/SSL traffic is not supported so you should

block that traffic as well.

See Default Handling Options for Undecryptable Traffic for more information about setting each option.

The following figure shows an example.

SSL Policy E	Example			
Rules Trusted	CA Certificates	Undecryptable Actions	Advand	ed Settings
Decryptio	n Errors Blog	ck	¥	
Handshak	e Errors Inhe	erit Default Action	Ŧ	
Session not	cached Inhe	erit Default Action	Ŧ	
Unsupported Ciph	er Suite	erit Default Action	*	
Unknown Ciph	er Suite	erit Default Action	Ŧ	
SSLv2	Session Blog	ck	•	
Compressed	Session Blog	ck	•	
		Revert to Defau	ults	

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

Step 12	Select the Enable TLS 1.3 Decryption check box. For more information about the other options, see Decryption
	Policy Advanced Options.

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
Advanced options are available only with Snort 3
Revert to Defaults

**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 20.

### **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.

Intrusion Prevention: Balanced Security and Connectivit 🔻 📼 🚦

• Enable logging.

#### Procedure

- **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**  $(\checkmark)$  next to your access control policy.
- **Step 4** (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.

٩		Decryption Policy	
	Name	Decryption Policy	
) v Ma	ndatory (1 - 1)	None	~
) (	<u> </u>	dr	Edit
√ De	fault	Create New Decryption Policy	

- b) From the list, click the name of your decryption policy.
- c) Click Apply.
- d) At the top of the page, click **Save**.
- Step 5From the Default Action list at the bottom of the page, click Intrusion Prevention: Balanced Security and<br/>Connectivity.

The following figure shows an example.

Default Action

- **Step 6** Click Logging ( $\blacksquare$ ).
- **Step 7** Select the **Log at End of Connection** check box and click **OK**.
- Step 8 Click Save.

#### What to do next

See Decryption Rule Examples, on page 8.

### **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.

Traffic to Prefilter, on page 9

First Decryption Rule: Do Not Decrypt Specific Traffic, on page 9

Next Decryption Rules: Decrypt Specific Test Traffic, on page 10

Do Not Decrypt Low-Risk Categories, Reputations, or Applications, on page 11

Create a Decrypt - Resign Rule for Categories, on page 12

Last Decryption Rules: Block or Monitor Certificates and Protocol Versions, on page 14

### **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

#### **Related Topics**

Prefiltering vs Access Control Best Practices for Fastpath Prefiltering

#### First Decryption Rule: Do Not Decrypt Specific Traffic

The first decryption 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.

Ru	les Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings								
									+ 4	dd Category	+ Add Rule	Q Search F	tules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Adn	ninistrator Rules												
Thi	is category is empty												
Star	ndard Rules												
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🕝 Do not d
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 Lou	any	any	any	any	🕑 Do not d
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	🕑 Do not
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	алу	Any (Except U	any	→ Decryp 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

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 sour	ce network									0
Name		Move								
	Enabled	below ru	Jle		• 1					
Action										
On not decrypt										
Zones Networks VLAN Tags	Users	Applications F	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
Available Networks C	+			Source Net	works (1)			Destination Net	works (0)	
Q Search by name or value				Intranet			Ì	any		
Networks Geolocation										
any IPv4-Private-All-RFC1918 any-ipv4 any-ipv6 defaultgateway insidesubnet Intranet IPv4-Benchmark-Tests				Enter an I	P address		Add	Enter an IP ac	ldress	Add
									Can	cel Save

### **Next Decryption 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.

	er Description												
R	ules Trusted CA Certificates	Undecryptat	le Actions	Advanced Se	ttings								
									+ Ad	d Category	+ Add Rule	Q Search F	Rules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Ad	Iministrator Rules												
	his category is empty												
Sta	andard Rules												
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	OD not decry
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	OD not decr
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot		any	any	any	🕑 Do not decr
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
Ro	ot Rules												

Rule detail:

ne								
ecrypt test site 🔽 Enab	led <u>Move</u>							
on								
Decrypt - Resign vith Into	A	- C 🔽 P	Replace Key Only	у				
ones Networks VLAN Tags User	s Applications Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
egories C	Reputations					Selected Categ	ories (1)	
Search by name or value	Any					Astrology (An	y reputation)	Ì
y (Except Uncategorized)	5 - Trusted							
ncategorized	4 - Favorable							
dult	3 - Neutral							
dvertisements	2 - Questionable							
cohol	1 - Untrusted							
nimals and Pets								
ts								
strology	Apply to unknown	reputation						
$ \langle$ $\langle$ Viewing 1-100 of 125 $\rangle$ $\rangle $								

### 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.

g Name Source Dest Source Dest Networks VLAN Use Administrator Rules This category is empty Standard Rules	Applicati	+ Add Category Source Ports Dest Port	+ Add Rule	Q Search R	Rules
a Namo Zones Zones Networks Networks Tags Use Administrator Fulges This category is empty	Applicati	Source Ports Dest Port	s Categories	SSL	
This category is empty					Action
Standard Rules					
1 DND internal source network any any any Intranet any any any	any	any any	any	any	🕝 Do not decr
2 Decrypt test site any any any any any any any	any	any any	Astrology (Any	y any	→ Decrypt - Resign
3 Do not decrypt low risk any any any any any any any	Risks: Very Lo	any any	any	any	OD not decr
4 Do not decrypt applications any any any any any any any	Facebook Facebook Mes Facebook Pho	any any	any	any	OD not dec
5 Decrypt all but trusted categ any any any any any any any any	any	any any	Any (Except U	h any	→ Decrypt - Resign
6 Block bad cert status any any any any any any any	any	any any	any	1 Cert Status se	Block
7 O Block SSLv3. TLS 1.0, 1.1 any any any any any any any	any	any any	any	3 Protocol Versi	Block
Root Rules					

Rule details:

Editing Rule - Do not decrypt lo	ow risk							0
Name								
Do not decrypt low risk	Enabled	Move						
Action								
OD not decrypt								
Zones Networks VLAN Tags	Users	Applications Ports	Category Ce	rtificate DN	Cert Status	Cipher Suite	Version	Logging
Application Filters C Clear A	II Filters	Available Applications (1483	)C			Selected Applica	tions and Filters (1)	
Q Search by name		Q. Search by name				Filters		
<ul> <li>Risks (Any Selected)</li> </ul>		050plus	0	Add to Ru		Risks:Very Low	, Low	Ŵ
Very Low	538	1&1 Internet	0					
Low	454	1-800-Flowers	0					
Medium	282	1000mercis	0					
High	139	12306.cn	0					
Very High	70	123Movies	0					
▼ Business Relevance (Any Selected	i)	126.com	0					
Very Low	580	17173.com	0					
		I< < Viewing 1-100	of 1483 > >					
							Cancel	Save
Add Dulo								~
Add Rule								0
Add Rule		Insert						0
	Enabled		•	Standard R	ules	¥		0
Name Do not decrypt applications Action	Enabled		v	Standard R	ules	¥		0
Name Do not decrypt applications	Enabled		•	Standard R	ules	×		0
Name Do not decrypt applications Action				Standard R	ules Cert Status	▼ Cipher Suite	Version	Cogging
Name Do not decrypt applications Action Do not decrypt Do not decrypt Zones Networks VLAN Tags	Users	into Category	Category Ce			Cipher Suite	Version ations and Filters (4)	
Name Do not decrypt applications Action Do not decrypt Do not decrypt Zones Networks VLAN Tags	Users	into Category Applications Ports	Category Ce			Cipher Suite		
Name Do not decrypt applications Action Construction Cons	Users	into Category Applications Ports Available Applications (0) (2)	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters		
Name Do not decrypt applications Action Do not decrypt Topology Cones Networks VLAN Tags Application Filters C Clear A Q, pinn	Users	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters	ations and Filters (4)	Logging
Name Do not decrypt applications Action Co Do not decrypt To Do not decrypt Cones Networks VLAN Tags Application Filters C Clear A C, pinn     Risks (Any Selected)	Users	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce	ations and Filters (4)	Logging
Name Do not decrypt applications Action Co Do not decrypt To Do not decrypt Co Do no	Users	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook Facebook Mess	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging
Name Do not decrypt applications Action Control Decrypt Cones Networks VLAN Tags Application Filters C Clear A Q pinn     Risks (Any Selected)    Business Relevance (Any Selected)    Types (Any Selected)   Cones Cone	Users	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging
Name Do not decrypt applications Action Do not decrypt Do not decrypt Cones Networks VLAN Tags Application Filters C Clear A Q pinn  Risks (Any Selected) U Business Relevance (Any Selected) U Categories (Any Selected) U Catego	Users	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook Facebook Mess	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging
Name Do not decrypt applications Action Do not decrypt Tones Networks VLAN Tags Application Filters C Clear A Q pinn    Risks (Any Selected)  VIAN Selected)  Categories (Any Selected)	Il Filters X X	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook Facebook Mess	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging
Name Do not decrypt applications Action Do not decrypt Tones Networks VLAN Tags Application Filters C Clear A Q pinn    Risks (Any Selected)  VIAN Selected)  Categories (Any Selected)	Il Filters X X	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook Facebook Mess	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging
Name Do not decrypt applications Action Do not decrypt Tones Networks VLAN Tags Application Filters C Clear A Q pinn    Risks (Any Selected)  VIAN Selected)  Categories (Any Selected)	Il Filters X X	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook Facebook Mess	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging
Name Do not decrypt applications Action Do not decrypt Tones Networks VLAN Tags Application Filters C Clear A Q pinn    Risks (Any Selected)  VIAN Selected)  Categories (Any Selected)	Il Filters X X	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook Facebook Mess	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging
Name Do not decrypt applications Action Do not decrypt Tones Networks VLAN Tags Application Filters C Clear A Q pinn    Risks (Any Selected)  VIAN Selected)  Categories (Any Selected)	Il Filters X X	Into Category Applications Ports Available Applications (0) C Q, faceb	Category Ce	rtificate DN	Cert Status	Cipher Suite Selected Applica Filters Tags:pinned ce Applications Facebook Facebook Mess	ations and Filters (4) ertificate <b>Filter:</b> "faceb" sage	Logging

Best Practices for Configuring Application Control Recommendations for Application Control

### **Create a Decrypt - Resign Rule for Categories**

This topic shows an example of creating a decryption 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.

L

#### Procedure

- 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** > **Decryption**.
- **Step 4** Click **Edit** (*I*) 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		Insert		
DR rule sample	Enabled	below rule	▼ 8	
Action				
🔂 Decrypt - Resign 🔹 🔻	with IntCA	• C	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.

lame								
Decrypt all except trusted cat Seable	ed <u>Move</u>							
ction								
☐ Decrypt - Resign    with IntCA	\ \	🔻 C 🔽 F	teplace Key Onl	y				
Zones Networks VLAN Tags Users	Applications Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
categories C	Reputations					Selected Categ	ories (1)	
Q Search by name or value	Any					Any (Except U	Incategorized) (R	eputations 1 🗑
Any (Except Uncategorized)	5 - Trusted							
Uncategorized	4 - Favorable							
Adult	3 - Neutral							
Advertisements	2 - Questionable							
Alcohol	1 - Untrusted							
Animals and Pets								
Arts								
Astrology	Apply to unknown	reputation						
I ≤ Viewing 1-100 of 125 > >						L		
1 Viewing 1-100 of 125 / /1								
							Ca	ncel Save

Internal Certificate Authority Objects

### Last 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.

Ru	les Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ttings								
									+ /	Add Category	+ Add Rule	Q Search F	tules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Adr	ninistrator Rules												
Thi	is category is empty												
Star	ndard Rules												
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	OD not dec
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	OD not dec
4	Do not decrypt applications	any	any	any	алу	any	алу	Facebook Facebook Mes Facebook Phot	any	any	any	any	🕑 Do not de
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
Roc	t Rules												
Thi	s category is empty												

#### Rule details:

ame												
Block bad cert status			Enabled	Move								
ction												
Block		•										
Zones Networks	VLAN	Tags	Users	Applications Ports	Categor	y C	Certificate	DN	Cert Status	Cipher Suite	Version	Loggin
Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any					Revert to Default
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any					
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any					
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any					
	Yes	No	Any	Server Mismatch:	Yes	No	Any					



Editing Rule - Block SSLv3. TI	_S 1.0								0
Name		Move							
Block SSLv3. TLS 1.0	Enabled	into Category		▼ St	andard R	ules	•		
Action									
Generation Block 🔹									
Zones Networks VLAN Tag	is Users App	lications Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
SSL v3.0									
TLS v1.0									
TLS v1.1									
TLS v1.2									
Revert to Defaults									
								Can	Save

Example: Decryption Rule to Monitor or Block Certificate Status, on page 15 Example: Decryption Rule to Monitor or Block Protocol Versions, on page 17 Optional Example: Decryption Rule to Monitor or Block Certificate Distinguished Name, on page 18

#### **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.



**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.

#### Procedure

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

- Step 2 Click Policies > Access Control > Decryption.
- **Step 3** Click **Edit** ( ) next to your SSL policy.
- **Step 4** Click **Edit** (*I*) 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 **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	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	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	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	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	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	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.



#### 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 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.

#### Procedure

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

Name		_									
Block SSLv3. TLS	1.0	Enabled	Move								
Action											
Block	•										
Zones Netwo	ks VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
SSL v3.0											
TLS v1.0											
TLS v1.1											
TLS v1.2											
Revert to Defaults											
										Cancel	Save

#### **Optional Example: 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 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; Distinguished Name (DN) Rule Conditions 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 > Decryption.
- **Step 3** Click **Edit** ( ) next to your SSL policy.

Step 10 Step 11

- **Step 4** Click **Edit** (*I*) 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 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)		Issuer DNs (1)	
GoodBakery		CN=goodca.example.com	Ĩ
Enter DN or CN	Add	Enter DN or CN	

# **Decryption Rule Settings**

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

decryption 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.)

#### Procedure

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 SSL policy.		
Step 4	Click Edit ( 🖍 ) next to a decryption rule.		
Step 5	Click the <b>Logging</b> tab.		
Step 6	Click Log at End of Connection.		
Step 7	Click Save.		
Step 8	Click <b>Save</b> at the top of the page.		