

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
- Recommended Policy and Rule Settings, on page 5
- Decryption Policy Walkthrough, on page 9

Decryption Rules Best Practices

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

Some general guidelines:

- Decrypting traffic requires processing and memory; decrypting too much traffic can impact performance. Before you set up decryption policies and rules, see When to Decrypt Traffic, When Not to Decrypt.
- Among the types of traffic you should exclude from decryption is traffic that is by nature undecryptable; typically, undecryptable traffic uses TLS/SSL certificate pinning.

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

SSL Policy Example

Enter [Description													
Rule	s Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings									
									+	Add Category	+ Add Rule	Q Search	Rules	>
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
Admi	nistrator Rules													
This	category is empty													
Stand	lard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Oo not decrypt	1
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign	/1
3	O not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	OD not decrypt	1
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	OD not decrypt	1
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt - Resign	1
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block	1
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	1
Root	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 or Secure Firewall 3100/4200 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 during evaluation period

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

Guidelines for undecryptable traffic

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

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 or undecryptable application filter

If you are decrypting traffic and you do not want users to see errors in their browsers when going to these sites, we recommend you set up a **Do Not Decrypt** rule toward the bottom of your decryption rules.

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

Name		Insert						
DND rule for pinned sites	Enabled	into Category	•	Standard Ru	les	Ŧ		
Action								
📀 Do not decrypt 🔹 👻								
Zones Networks VLAN Tage	Users	Applications Ports	Category Certific	ate DN	Cert Status	Cipher Suite	Version	Log
Application Filters C Clear	NI Filters 🗙	Available Applications (40)	2			Selected Applie	cations and Filters (0)	
Q pin	×	Q Search by name				any		
 Risks (Any Selected) 		All apps matching the filter		Add to Rul	e			
 Business Relevance (Any Selected 	(b	Airbnb	0					
▼ Types (Any Selected)		Apple Mail	0					
 Categories (Any Selected) 		Chase	0					
▼ Tags (1 Selected)		Dropbox	0					
🕨 🗹 pinned certificate	40	Gmail	0					
		Google	0					
		Google Accounts Authentic	cation 0					

Decrypt - Resign and Decrypt - Known Key Best Practices

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

Do not use Version or Cipher Suite rule conditions



Important Never use either Cipher Suite or Version rule conditions in a rule with a Decrypt - Resign or Decrypt - Known Key rule action. The use of these conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

Decrypt - Resign best practices with certificate pinning

Some applications use a technique referred to as *TLS/SSL pinning* or *certificate pinning*, which embeds the fingerprint of the original server certificate in the application itself. As a result, if you configured a decryption rule with a **Decrypt - Resign** action, when the application receives a resigned certificate from a managed device, validation fails and the connection is aborted.

Because TLS/SSL pinning is used to avoid man-in-the-middle attacks, there is no way to prevent or work around it. We recommend adding a Do Not Decrypt rule before the **Decrypt - Resign** rule so pinning traffic is excluded from being decrypted.

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 either a destination network to the TBD rule rules (**Networks** rule condition) or add a security zone to the access control rule (**Zones** tab page). That way the traffic goes directly to the network or interface on which the server is located, thereby reducing traffic on the network.

Decryption Rules to Put First

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

Decryption Rules to Put Last

Rules with the following rule conditions should be ordered immediately 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

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 rules: Enable logging for every rule except those with a **Do Not Decrypt** rule action. (It's up to you; if you want to see information about traffic that isn't decrypted, enable logging for those rules also.)
- Access control policy:
 - Associate your decryption policy with an access control policy. (If you fail to do this, your decryption policy and rules have no effect.)
 - Set the default policy action to Intrusion Prevention: Balanced Security and Connectivity.
 - Enable logging.

Related Topics

Decryption Policy Settings, on page 6 Decryption Rule Settings, on page 26 Access Control Policy Settings, on page 8

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 rules: Enable logging for every rule except those with a **Do Not Decrypt** rule action. (It's up to you; if you want to see information about traffic that isn't decrypted, enable logging for those rules also.)
- Access control policy:
 - Associate your decryption policy with an access control policy. (If you fail to do this, your decryption policy and rules have no effect.)

- Set the default policy action to Intrusion Prevention: Balanced Security and Connectivity.
- Enable logging.

Related Topics

Decryption Policy Settings, on page 6 Decryption Rule Settings, on page 26 Access Control Policy Settings, on page 8

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 Step 3	Click Policies > Access (Click Edit () next to ye From the Default Action The following figure show	Control > Decryption. our decryption policy. I list at the bottom of the page, ws an example.	click Do Not Decrypt .	
	Default Action		Do not decrypt	~ E
Step 4	At the end of the row, clic	ck Logging (
Step 5	Select the Log at End of	Connection check box.		
	The following figure show	ws an example.		
	Logging	0		
	✓ Log at End of Connection			
	Send Connection Events to:			
	Firewall Management Center			
	Using default syslog configuration in Ac	ccess Control Logging)		
	Show Overrides			
	SNMP Trap			
	Select an SNMP Alert Configu	· +		
		Cancel		

Step 6 Click OK.

Step 7 Click Save.

Step 8 Click the Undecryptable Actions tab.

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

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

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

The following figure shows an example.

SSL Policy Example	e	
Rules Trusted CA Certific	ates Undecryptable Actions	Advanced Settings
Decryption Errors	Block	v
Handshake Errors	Inherit Default Action	v
Session not cached	Inherit Default Action	•
Unsupported Cipher Suite	Inherit Default Action	•
Unknown Cipher Suite	Inherit Default Action	•
SSLv2 Session	Block	•
Compressed Session	Block	•
	Revert to Defau	ults

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

Step 11 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 12 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 26.

Access Control Policy Settings

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

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

Procedure

- Step 1 Click Policies > Access Control.
- **Step 2** Click **Edit** (*I*) next to your access control policy.
- **Step 3** (If your decryption policy is not set up yet, you can do this later.)
 - a) Click the **Decryption** link at the top of the page as the following figure shows.

٩		Decryption Policy	
)	Name	Decryption Policy	
) v Manda	tory (1-1)	None	~
		dr	Edit

- b) From the list, click the name of your decryption policy.
- c) Click Apply.
- d) At the top of the page, click Save.
- **Step 4** From the **Default Action** list at the bottom of the page, click **Intrusion Prevention: Balanced Security and Connectivity**.

The following figure shows an example.

Default Action

Intrusion Prevention: Balanced Security and Connectivit 🔻 📼 🖺

- **Step 5** Click Logging (\blacksquare).
- **Step 6** Select the **Log at End of Connection** check box and click **OK**.
- Step 7 Click Save.

What to do next

See Decryption Rule Examples, on page 13.

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.

Number Number Advanced Beeting Number Number Advanced Beeting Number Number Advanced Beeting Number Advanced Beeting Source Destance Number Source Source Destance Number Restore Source Destance Number Restore Source Destance Source Source Destance Number Restore Source Destance Restore Source Restore Restore </th <th>SSL Enter I</th> <th>Policy Example</th> <th></th> <th>Save</th> <th>Cancel</th>	SSL Enter I	Policy Example												Save	Cancel
$ \begin the term of term$	Rule	rusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings									
image Name Date Name VacaN Applicable Sporte Destores State of Action All interview Calles Calles Calles Sectores Sectore Sectore Sectore Sectore Sectore Sectore Sectore										+ /	Add Category	+ Add Rule	् Search F	≀ules	×
Advances Serve of the s	#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
This satisfy the state of	Admi	inistrator Rules													
Statistical Source network any	This	category is empty													
1 DND Internal source network any <	Stand	dard Rules													
2 Decrypt test site any any <td>1</td> <td>DND internal source network</td> <td>any</td> <td>any</td> <td>Intranet</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>🕑 Do not decrypt</td> <td>1</td>	1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🕑 Do not decrypt	1
3 \bullet Do not decrypt low risk any any any any any any any any \bullet Do not decrypt \bullet 4 Do not decrypt applications any any any any any any any \bullet Do not decrypt \bullet 5 Decrypt all but trusted categ any any any any any any \bullet Decrypt \bullet \bullet 6 \bullet Block bad cert status any any any any any \bullet Decrypt \bullet \bullet 7 \bullet Block SSLv3. TLS 1.0, 1.1 any any any any any any \bullet Decrypt \bullet \bullet This category is empty: Decrypt \bullet \bullet Decrypt \bullet \bullet Decrypt \bullet <td>2</td> <td>Decrypt test site</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>any</td> <td>Astrology (Any</td> <td>any</td> <td>→ Decrypt - Resign</td> <td>/1</td>	2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign	/1
4 Do not decrypt applications any <	3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	OD not decrypt	1
5 Decrypt all but trusted categ any any any any any any any Any (Except) any $\frac{1}{Reign}$	4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	⊘Do not decrypt	/1
6 • Block bad cert status any an	5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt - Resign	/1
7 Block SSLv3. TLS 1.0, 1.1 any	6	 Block bad cert status 	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block	/=
Root Rules This category is empty Default Action Do not decrypt	7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	1
Default Action Do not decrypt Image: Constraint of the cons	Root	Rules													
Default Action Do not decrypt 🔹 📱	This	category is empty													
	Defa	ult Action											Do not decrypt		- 8

See one of the following sections for more information.

Related Topics

Recommended Policy and Rule Settings, on page 5 Traffic to Prefilter, on page 13 First Decryption Rule: Do Not Decrypt Specific Traffic, on page 14 Next Decryption Rules: Decrypt Specific Test Traffic, on page 15 Create a Decrypt - Resign Rule for Categories, on page 18 Do Not Decrypt Low-Risk Categories, Reputations, or Applications, on page 16 Decryption Rules: Block or Monitor Certificates and Protocol Versions, on page 19

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 rules: Enable logging for every rule except those with a **Do Not Decrypt** rule action. (It's up to you; if you want to see information about traffic that isn't decrypted, enable logging for those rules also.)
- · Access control policy:
 - Associate your decryption policy with an access control policy. (If you fail to do this, your decryption policy and rules have no effect.)
 - Set the default policy action to Intrusion Prevention: Balanced Security and Connectivity.
 - Enable logging.

Related Topics

Decryption Policy Settings, on page 6 Decryption Rule Settings, on page 26 Access Control Policy Settings, on page 8

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	Click Policies > Access Control > Decryption .						
Step 2 Step 3	Click Edit () next to your decryption policy. 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 v					
Step 4	At the end of the row, click Logging (

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

The following figure shows an example.

 Log at End of Connection Send Connection Events to: Firewall Management Center Syslog Server (Using default syslog configuration in Access Control Loggi Show Overrides SNMP Trap 		(?)
Send Connection Events to: Firewall Management Center Syslog Server (Using default syslog configuration in Access Control Loggi Show Overrides SNMP Trap		
Firewall Management Center Syslog Server Using default syslog configuration in Access Control Loggi Show Overrides SNMP Trap		
Syslog Server Using default syslog configuration in Access Control Loggi Show Overrides SNMP Trap		
SNMP Trap	in Access (Control Logging)
Select an SNMP Alert Configu~ +	guv -	÷
Select an SNMP Alert Config		in Access C

- Step 6 Click OK.
- Step 7 Click Save.
- Step 8 Click the Undecryptable Actions tab.
- **Step 9** We recommend setting the action for **SSLv2 Session** and **Compressed Session** to **Block**.

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

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

The following figure shows an example.

SSL Policy Example	9	
Rules Trusted CA Certifica	ates Undecryptable Actions	Advanced Settings
Decryption Errors	Block	v
Handshake Errors	Inherit Default Action	•
Session not cached	Inherit Default Action	¥
Unsupported Cipher Suite	Inherit Default Action	•
Unknown Cipher Suite	Inherit Default Action	v
SSLv2 Session	Block	•
Compressed Session	Block	•
	Revert to Defau	ilts

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

Step 11 Select the **Enable TLS 1.3 Decryption** check box. For more information about the other options, see Decryption Policy Advanced Options.

Applies to	0 7.1.0 and later
	ock flows requesting ESNI
	sable HTTP/3 advertisement
C Pr	opagate untrusted server certificates to clients
Applies to	o 7.2.0 and later
C En	able TLS 1.3 Decryption
Applies to	o 7.3.0 and later
C En	able adaptive TLS server identity probe
Advanced	d options are available only with Snort 3
	Revert to Defaults

Step 12 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 26.

Access Control Policy Settings

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

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

Procedure

- Step 1 Click Policies > Access Control.
- **Step 2** Click Edit (\checkmark) next to your access control policy.
- **Step 3** (If your decryption policy is not set up yet, you can do this later.)
 - a) Click the **Decryption** link at the top of the page as the following figure shows.

Packets	→ Ø Prefilter Rule	Is → ○ Decryption → Security Integration	elligence → 🥑 Identity -
T Q		Decryption Policy	0
	Name	Decryption Policy	
∨ Ma	Indatory (1 - 1)	dr	Edit
✓ De There	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 4** From the **Default Action** list at the bottom of the page, click **Intrusion Prevention: Balanced Security and Connectivity**.

The following figure shows an example.

Intrusion Prevention: Balanced Security and Connectivit 💌 📼 🚆

Step 5 Click Logging (\blacksquare).

Default Action

- **Step 6** Select the **Log at End of Connection** check box and click **OK**.
- Step 7 Click Save.

What to do next

See Decryption Rule Examples, on page 13.

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.

Related Topics

Traffic to Prefilter, on page 13 First Decryption Rule: Do Not Decrypt Specific Traffic, on page 14 Next Decryption Rules: Decrypt Specific Test Traffic, on page 15 Do Not Decrypt Low-Risk Categories, Reputations, or Applications, on page 16 Create a Decrypt - Resign Rule for Categories, on page 18 Decryption Rules: Block or Monitor Certificates and Protocol Versions, on page 19

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.

	SSL Enter (Policy Example												Save	Cancel
	Rule	s Trusted CA Certificates I	Undecryptable	e Actions	Advanced Sett	ings									
										+ Ade	d Category	+ Add Rule	Q Search F	ules:	×
		Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
	Admi	nistrator Rules													
	This	category is empty													
	Stand	fard Rules													
\rightarrow	1	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	/1
	3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	OD not decrypt	/1
	4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	OD not decrypt	/1
	5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt - Resign	/1
	6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block	1
	7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	/1
	Root	Rules													
	This	category is empty													
	Defa	ult Action											Do not decrypt		•



Note

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

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

Rule detail:

me		Move				
OND internal source network	Enabled	below rule	v 1			
tion						
🔊 Do not decrypt 🗸 🔻	•					
Zones Networks VLAN T	ags Users	Applications Ports	Category Certificate DI	N Cert Status	Cipher Suite Version	Logging
ailable Networks C	+		Source Networks (1)		Destination Networks (0)	
Search by name or value			Intranet	Ì	any	
letworks Geolocation						
ny						
v4-Private-All-RFC1918						
ny-ipv4						
ny-ipv6						
efaultgateway						
sidesubnet						
tranet			Enter an IP address	Add	Enter an IP address	Add
Pv4-Benchmark-Tests						

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.

	Enter [Description												Save	Cancel
	Rule	s Trusted CA Certificates	Undecryptable	e Actions	Advanced Sett	ings									
										+	Add 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	
	Admi	nistrator Rules													
	This	category is empty													
	Stand	lard Rules													
	1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	OD not decrypt	/1
\rightarrow	2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign	/1
	3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lov	any	any	any	any	OD not decrypt	11
	4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	🕑 Do not decrypt	/1
	5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt - Resign	/1
	6	Block bad cert status	any	any	any	any	any	any	any	any	алу	any	1 Cert Status se	Block	/1
	7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block	/1
	Root	Rules													
	This	category is empty													
	Defa	ult Action											Do not decrypt		* B

Rule detail:

Decrypt test site Decrypt test	lame											
ategories C Becryst - Resign with IntCA Category Certificate DN Cert Status Cipher Sule Version Logger ategories C Search by name or value Advit aname	Decrypt test site		Enabled	Move								
Percypt - Resign	ction											
Zene Network VLAN Tags Users Applications Pers Category Certificate DN Cert Status Cipher Suite Version Loggr aterportes C Reputations Accord Incategorized Addit Incategorized Addit Incategorized Addit Incategorized Addit Actord Animals and Pres Atasis Actord Antional status If < Version If <	🚰 Decrypt - Resign	▼ with	IntCA		•	C 🔽 Rep	lace Key Only					
tetepories C A search by name or value Active Block Active Block Active Block Active Block Active Block Active Block Active Block Active Block Active Block Active Block Active Bl	Zones Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Loggir
A seach by name or value Ary (Escept Uncategorized) Ary (Escept Uncategorized) Addit Action Bude Action Action Bude Action Actio	ategories C			Reputations						Selected Cate	gories (1)	
Any (Except Uncategorized) Aduit Advertisements Actively and Pers Active Akardogy Active Akardogy Concell 125 >>1 Cancell 125 Active	Search by name or value			Any						Astrology (A	ny reputation)	
Uncategorized Aduit Aduit Advertisements Actorolo Animals and Pets Arts Astology Astrology Astrology I - 100 of 125 >>1 Cancell © Apply to unknown reputation I < C Viewing 1-100 of 125 >>1 Cancell © S Cancell © S	Any (Except Uncategorized	i)		5 - Trusted								
Adudt Advertisements Advended Adve	Uncategorized											
Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Acohol Advertisements Cencel	Adult											
Alcohol Animals and Pets Ats Astrology IC < Viewing 1-100 of 125 >>1 Cancel Str Cancel Str Canc	Advertisements											
Animais and Pets Arts Astrology IC < Viewing 1-100 of 125 >>1 Cancel State Action Selected Categories (1) Cancel State Action Cancel State Cancel St	Alcohol											
Arts Astrology IC < Viewing 1-100 of 125 > XI Cancel Sin Add Rule are insert Decrypt test site Plabled below rule S Selected Categories (1) Ary (Secept Uncategorized) Astrology Ary (Except Uncategorized) Astrology Ary (Except Uncategorized) Astrology Ary (Except Uncategorized) Astrology And to Rule C Questionable 1 - Untrusted C Questionable 1 - Untrusted C Questionable C QUESTIONA C QUESTIONA	Animals and Pets											
Astrology I < Viewing 1-100 of 125 >>1 Cancel Sav Add Rule are Insert Decrypt - Resign with IntCA Category Certificate DN Cert Status Cipher Suite Version Logg ategories C Ary S - Trusted - Favorable - S - Trusted - S - Neutral - Certificate Categories C Ary S - Trusted - S - Neutral - Certificate Categories C Ary S - Trusted - S - Neutral - Certificate Categories C Ary S - Trusted - S - Neutral - Certificate Categories C Ary S - Trusted - S - Neutral - Certificate Categories C Ary S - Trusted - S - Neutral - Certificate Categories C Ary S - Trusted - S - Neutral - Certificate Categories C Ary C - Certificate Categories	Arts											
Add Rule ame Insert Decrypt test site Enabled below rule S Decrypt - Resign with IntCA C Replace Key Only ones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logg Atorology (Any reputation) Add to Rule 1 Favorable 3 Neutral 2 Questionable 1 Untrusted Version 2 Questionable 1 Untrusted	Astrology			Apply to ur	oknown reni	itation						
ame Insert Decrypt test site Finabled below rule	IC C Viewing 1-100	0 of 125 >>1									Can	cel Sav
Decrypt test site Decrypt test site Decrypt - Resign Multi IntCA C Replace Key Only ones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logs ategories C Reputations Selected Categories (1) Astrology (Any reputation) Selected Categories (1) Astrology (Any reputation) Astrology (Any	Add Rule	0 of 125 >>1									Can	cel Sav
tion Decrypt - Resign with IntCA C Replace Key Only ones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status ▲ Cipher Suite ▲ Version Logg tegories C Reputations Selected Categories (1) Astrology (Any reputation) S - Trusted 4 - Favorable 3 - Neutral 2 - Questionable 1 - Untrusted Vapply to unknown reputation	IK < Viewing 1-100	0 of 125 >>1		Insert							Can	cel Sav
Decrypt - Resign vith IntCA v C Peplace Key Only ones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logs tegories C Reputations Astrology Infrastructure and Content Delivery Netw Apply to unknown reputation Apply to unknown reputation	Add Rule	0 of 125 >>1	Enabled	Insert Delow	rule		× 5				Can	cel Sav
Ones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logs ategories C* Reputations Selected Categories (1) Astrology (Any reputation) Astrology (Any reputation) Astrology Infrastructure and Content Delivery Netw 3 - Neutral 2 - Questionable 1 - Untrusted	Add Rule ame Decrypt test site ttion) of 125 >>1	Enabled	Insert below	rule		× 5				Can	cel Sav
ategories C* Reputations Selected Categories (1) Any Any 5 - Trusted Astrology (Any reputation) Astrology 3 - Neutral 2 - Questionable 1 - Untrusted 1 - Untrusted Y Apply to unknown reputation Y Apply to unknown reputation	Add Rule ame Decrypt test site tion Decrypt - Resign	∑ with	Enabled IntCA	Insert below	rule	C 🔽 Rep	✓ 5 place Key Only				Can	Cei Sav
Q. astr Any Any (Except Uncategorized) 5 - Trusted Astrology 4 - Favorable 3 - Neutral 2 - Questionable 1 - Untrusted - Untrusted	I< < Viewing 1-100 Add Rule ame Decrypt test site tition	or 125 >>> vith AN Tags Us	Enabled IntCA	Insert below	rule v ts Cate	C° 🔽 Reg gory Certi	✓ 5 place Key Only iffcate DN	Cert	• Status	Cipher Suite	Can	Ceel Sav
Any (Except Uncategorized) Astrology Infrastructure and Content Delivery Netw 5 - Trusted 4 - Favorable 3 - Neutral 2 - Questionable 1 - Untrusted Add to Rule	Add Rule ame Decrypt test site ction Decrypt - Resign ones Networks VL ategories C	v with AN Tags U:	Enabled IntCA sers Ap	Insert below uplications Por	rule v ts Cate	C Z Reg gory Certi	× 5 place Key Only ificate DN	y Cert	Status	Cipher Suite Selected Cate	Can Version gories (1)	Ccel Sav
Astrology Astrology Infrastructure and Content Delivery Netw 2 - Questionable 1 - Untrusted Apply to unknown reputation	Add Rule ame Decrypt test site ction ame Decrypt - Resign ones Networks VL ategories C ^a Q. astr	v with	Enabled IntCA sers Ap	Insert below plications Por eputations Any	rule v ts Cate	C V Reg gory Certi	✓ 5 place Key Only ificate DN	Cert	Status	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	Ccel Sav
3 - Neutral 2 - Questionable 1 - Untrusted	Add Rule ame Decrypt test site ction Gerypt - Resign ones Networks VL ategories C ^o Q astr Any (Except Uncategories)	→ with AN Tags U:	Enabled IntCA Sers Ap	Insert below pulications Por putations Any 5 - Trusted	rule v ts Cate	C' 🔽 Reg gory Certi	✓ 5 place Key Only fficate DN	y Cert	Status	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	cei Sav
2 - Questionable 1 - Untrusted	Add Rule ame Decrypt test site ction Decrypt - Resign ones Networks VL ategories C ^a Q astr Any (Except Uncategorized	or f 125 >> v th AN Tags Us	Enabled IntCA sers Ap	Insert below splications Por sputations Any 5 - Trusted 4 - Favorable	rule v ts Cate	C' 🔽 Reg gory Certi	✓ 5 place Key Only ificate DN	y Cert	. Status	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	cei Sav
 1 - Untrusted ✓ Apply to unknown reputation 	Add Rule ame Decrypt test site ction Decrypt - Resign ones Networks VL ategories C [*] Q astr Any (Except Uncategorizet Astrology Infrastructure and Content	with AN Tags U: Delivary Methy	Enabled IntCA sers Ap	Insert below pplications Por oputations 5 - Trusted 4 - Favorable 3 - Neutral	rule 	C° 🔽 Reg gory Certi	× 5 place Key Only ificate DN	y Cert to Rule	Status	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	Cei Sav
Apply to unknown reputation	Add Rule ame Decrypt test site ction Cones Networks VL ategories C Q astr Any (Except Uncategorized Astrology Infrastructure and Content	with AN Tags U: Delivery Netw.	Enabled IntCA sers Ap	Insert below opplications Por opputations Any 5 - Trusted 4 - Favorable 3 - Neutral 2 - Questionable	rule v ts Cate	C° 🔽 Reg gory Certi	✓ 5 place Key Only fficate DN	y Cert to Rule	Status 🛕	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	Cel Sav
Apply to unknown reputation	Add Rule Add Rule Iame Decrypt test site Ction Cones Networks VL ategories C astr Any (Except Uncategorized Astrology Infrastructure and Content	v vith AN Tags U: v	Enabled IntCA sers Ap	Insert below pplications Por putations Any 5 - Trusted 4 - Favorable 3 - Neutral 2 - Questionable 1 - Untrusted	rule V ts Cate	C' 🗸 Reg gory Certi	✓ 5 place Key Only ificate DN	y Cert	Status	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	Cel Sav
Apply to unknown reputation	Add Rule Add Rule Imme Decrypt test site ction Decrypt - Resign Cones Networks VL ategories C Q astr Any (Except Uncategorized Astrology Infrastructure and Content	v vith AN Tags U: d) Delivery Netw.	Enabled IntCA sers Ap	Insert below epitations Por eputations 5 - Trusted 4 - Favorable 3 - Neutral 2 - Questionable 1 - Untrusted	rule × ts Cate	C' 🗸 Reg gory Certi	 ✓ 5 place Key Only ificate DN Add 	y Cert	Status	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	Cel Sav
	Add Rule Add Rule Imme Decrypt test site ction Decrypt - Resign Cones Networks VL ategories C Q astr Any (Except Uncategorized Astrology Infrastructure and Content	v vith AN Tags U: v	Enabled IntCA sers Ap	Insert below epitations Por eputations 5 - Trusted 4 - Favorable 3 - Neutral 2 - Questionable 1 - Untrusted	rule v ts Cate	C' 🗸 Reg gory Certi	 ✓ 5 place Key Only ificate DN Add 	y Cert	Status	Cipher Suite Selected Cate Astrology (A	Version gories (1) ny reputation)	Logg

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.

_		Undecrypta	DIe Actions	Advanced Se	ettings								
									+	Add Category	+ Add Rule	Q Search I	Rules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Adr	ninistrator Rules												
Th	is category is empty												
Sta	ndard Rules												
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🕗 Do not de
2	Decrypt test site	anγ	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	апу	any	any	any	Risks: Very Lov	any	any	any	any	🕑 Do not de
4	Do not decrypt applications	any	any	any	any	any	any	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 U	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

Rule details:

Editing Rule - Do not decrypt low risk				0
Name Do not decrypt low risk Con	d <u>Move</u>			
Zones Networks VLAN Tags Users	Applications Ports Cate	gory Certificate DN Cert Status	Cipher Suite Version	Logging
Application Filters C Clear All Filters	Available Applications (1483) C		Selected Applications and Filters (1)	
Q Search by name	Q Search by name		Filters	
 Risks (Any Selected) 	050plus	Add to Rule	Risks:Very Low, Low	Ì
Very Low 538	1&1 Internet	•		
Low 454	1-800-Flowers	0		
Medium 282	1000mercis	0		
High 139	12306.cn	0		
Very High 70	123Movies	0		
 Business Relevance (Any Selected) 	126.com	0		
Very Low 580	17173.com	0		
	I ≤ Viewing 1-100 of 148	33 > >		

Cancel Save

Name Insert Do not decrypt applications Enabled into Category Action C Do not decrypt	Add Rule						0
	Name Do not decrypt applications Action On to decrypt	Enabled	Insert into Category	•	Standard Rules	×	
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging	Zones Networks VLAN Tags	Users	Applications Ports	Category Certificate	e DN Cert Status	Cipher Suite Version	Logging
Application Filters C Clear All Filters X Available Applications (0) C Selected Applications and Filters (4) Q pinn Q faceb X • Risks (Any Selected) All apps matching the filter Add to Rule Filters • Risks (Any Selected) All apps matching the filter Add to Rule Filters • Categories (Any Selected) • Categories (Any Selected) Filters Facebook • Tags (1 Selected) • Tags (1 Selected) • Facebook Message • Facebook Photos • pinned certificate 0 • Implications • Implications	Application Filters C Clear A Q. pinn Itsks (Any Selected) • Risks (Any Selected) • Types (Any Selected) • Categories (Any Selected) • Tags (1 Selected) • Tags (1 Selected) • Tags (1 Selected)	I Filters X Au	vailable Applications (0) @ 2, faceb	X		Selected Applications and Filters (4) Filters Tags:pinned certificate Filter:"faceb" Applications Facebook Facebook Message Facebook Photos	() () ()

Related Topics

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.

Procedure

Step 1	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 2	Click Policies > Access Control > Decryption.
Step 3	Click Edit () next to your decryption policy.
Step 4	Click Add Rule.
Step 5	In the Name field, enter a name to identify the rule.
Step 6	From the Action list, click Decrypt - Resign.
Step 7	From the with list, click the name of your internal CA.
Step 8	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 9** Click the **Category** tab page.
- **Step 10** From the top of the **Categories** list, click **Any** (**Except Uncategorized**).
- **Step 11** From the **Reputations** list, click **Any**.
- Step 12 Click Add to Rule.

The following figure shows an example.

ame							
Decrypt all except trusted cat Zenabled	Move						
ction							
Decrypt - Resign vith IntCA	•	ී 🔽 Replace Key 0	Only				
Zones Networks VLAN Tags Users	Applications Ports	Category Certificate	e DN C	ert Status	Cipher Suite	Version	Loggin
ategories C	Reputations				Selected Categ	ories (1)	
ৎ, Search by name or value	Any				Any (Except U	Incategorized) (Re	putations 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 re	putation					
< < Viewing 1-100 of 125 >>							
-							

Related Topics

Internal Certificate Authority Objects

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	Iles Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings								
									+ Ac	dd Category	+ Add Rule	Q Search	Rules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Ad	ministrator Rules												
Th	is category is empty												
Sta	indard 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 Lo	any	any	any	any	OD not o
4	Do not decrypt applications	any	any	any	алу	any	any	Facebook Facebook Mes Facebook Pho	any	any	any	any	🕑 Do not e
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	any	→ Decrypt Resign
6	Block bad cert status	any	any	any	алу	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

Rule details:

Editing Rule - Block	bad ce	ert sta	atus									0
Name												
Block bad cert status			Enabled	Move								
Action												
Block		•										
Zones Networks	VLAN	Tags	Users	Applications Ports	Catego	y	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
Revoked:	Yes	No	Any	Self Signe	d: Yes	No	Any					Revert to Defaults
Valid:	Yes	No	Any	Invalid Signatur	e: Yes	No	Any					
Invalid Issuer:	Yes	No	Any	Expire	d: Yes	No	Any					
Not Yet Valid:	Yes	No	Any	Invalid Certificat	e: Yes	No	Any					
Invalid CRL:	Yes	No	Any	Server Mismatc	h: Yes	No	Any					
	(3) (1) (1)											



Editing Rule - Block SSLv3	. TLS 1.0						0
Name		Move					
Block SSLv3. TLS 1.0	Enabled	into Category	•	Standard Rules	•		
Action							
Block	•						
Zones Networks VLAN	Tags Users Applic	ations Ports Ca	Category Certificate	e DN Cert Sta	tus Cipher Suite	Version	Logging
SSL v3.0							
TLS v1.0							
TLS v1.1							
TLS v1.2							
Revert to Defaults							
						Cancel	Save

Related Topics

Example: Decryption Rule to Monitor or Block Certificate Status, on page 21 Example: Decryption Rule to Monitor or Block Protocol Versions, on page 23 Optional Example: Manual Decryption Rule to Monitor or Block Certificate Distinguished Name, on page 24

Example: Decryption Rule to Monitor or Block Certificate Status

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



Important

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

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 decryption policy.

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

- Click **Edit** (*I*) next to a decryption rule. Step 4
- Step 5 Click Add Rule.
- Step 6 n the Add Rule dialog box, in the Name field, enter a name for the rule.
- Step 7 Click Cert Status.
- Step 8 For each certificate status, you have the following options:
 - Click Yes to match against the *presence* of that certificate status.

- Click No to match against the *absence* of that certificate status.
- Click **Any** to skip the condition when matching the rule. In other words, choosing **Any** means the rule matches whether the certificate status is present or absent.
- **Step 9** From the **Action** list, click either **Monitor** to only monitor and log traffic that matches the rule or click **Block** or **Block with Reset** to block the traffic and optionally reset the connection.
- **Step 10** To save changes to the rule, at the bottom of the page, click **Add**.
- **Step 11** To save changes to the policy, at the top of the page, click **Save**.

Example

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

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

Revoked:	Yes	No	Any	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.

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.

					1						
Revoked:		Yes	No	Any		Se	lf Sig	ned:	Yes	No	Any
Valid:		Yes	No	Any	In	valid S	Signa	ture:	Yes	No	Any
Invalid Issuer:		Yes	No	Any			Exp	ired:	Yes	No	Any
Not Yet Valid:		Yes	No	Any	Inv	alid C	ertifi	cate:	Yes	No	Any
Invalid CRL:		Yes	No	Any	Se	erver N	lism	atch:	Yes	No	Any
Revoked:	Yes	No	Any		Self Signed:	Yes	No	Any			
Valid:	Yes	No	Any	li	nvalid Signature:	Yes	No	Any			
Invalid Issuer:	Yes	No	Any		Expired:	Yes	No	Any			
Not Yet Valid:	Yes	No	Any	In	valid Certificate:	Yes	No	Any			
Invalid CRL:	Yes	No	Any	S	erver 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 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.



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	Click Policies > Access Control > Decryption .
Step 2	Click Edit () next to your decryption policy.
Step 3	Click Edit () next to a decryption rule.
Step 4	Click Add Rule.
Step 5	In the Add Rule dialog box, in the Name field, enter a name for the rule.
Step 6	From the Action list, click Block or Block with reset.
Step 7	Click Version page.
Step 8	Check the check boxes for protocols that are no longer secure, such as SSL v3.0 , TLS 1.0 , and TLS 1.1 . Clear the check boxes for any protocols that are still considered secure.

The following figure shows an example.

Block SSI	Lv3. TLS 1.0		Enabled	Move								
ction	2001 120 110			intere								
Block		•										
Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Loggin
SSL v3	3.0											
TLS v1	.0											
TLS v1	.1											
TLS v1	.2											
Revert to	Defaults											
											Cancel	Sav

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

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

The distinguished name can consist of country code, common name, organization, and organizational unit, but typically consists of a common name only. For example, the common name in the certificate for https://www.cisco.com is cisco.com. (However, it's not always this simple; Distinguished Name (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

Step 9 Step 10 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	Click Policies > Access Control > Decryption.
Step 2	Click Edit (🖍) next to your decryption policy.
Step 3	Click Edit () next to a decryption rule.
Step 4	Click Add Rule.
Step 5	In the Add Rule dialog box, in the Name field, enter a name for the rule.
Step 6	From the Action list, click Block or Block with reset.
Step 7	Click DN .
Step 8	Find the distinguished names you want to add from the Available DNs, as follows:
	• To add a distinguished name object on the fly, which you can then add to the condition, click Add (+) above the Available DNs list.
	• To search for distinguished name objects and groups to add, click the Search by name or value prompt above the Available DNs list, then type either the name of the object, or a value in the object. The list updates as you type to display matching objects.
Step 9	To select an object, click it. To select all objects, right-click and then Select All.
Step 10	Click Add to Subject or Add to Issuer.
	TipYou can also drag and drop selected objects.
Step 11	Add any literal common names or distinguished names that you want to specify manually. Click the Enter DN or CN prompt below the Subject DNs or Issuer DNs list; then type a common name or distinguished name and click Add .
	Although you can add a CN or DN to either list, it's more common to add them to the Subject DNs list.
Step 12	Add or continue editing the rule.
Step 13	When you're done, to save changes to the rule, click Add at the bottom of the page.
Step 14	To save changes to the policy, click Save at the top of the page.

Example

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

Subject DNs (1)		Issuer DNs (1)	
GoodBakery		CN=goodca.example.com	Ì
Enter DN or CN	Add	Enter DN or CN Add	

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

	Click Policies > Access Control > Decryption .
2	Click Edit () next to your decryption policy.
	Click Edit (🖍) next to a decryption rule.
	Click the Logging tab.
	Click Log at End of Connection.
	Click Save.
	Click Save at the top of the page.