cisco.



TLS/SSL 7.2 ルールの展開と例

初版:2022年2月22日 最終更新:2022年11月21日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー http://www.cisco.com/jp お問い合わせ先:シスココンタクトセンター 0120-092-255 (フリーコール、携帯・PHS含む) 電話受付時間:平日10:00~12:00、13:00~17:00 http://www.cisco.com/jp/go/contactcenter/





第1章 TLS/SSL ルール ベスト プラクティス 1 TLS/SSL ルール ベスト プラクティス 1 プレフィルタとフローオフロードによる検査のバイパス 2 [復号しない(Do Not Decrypt)]のベストプラクティス 3 [復号-再署名(Decrypt - Resign)]と[復号-既知のキー(Decrypt - Known Key)]のベストプ ラクティス 4 最初に配置する TLS/SSL ルール 4 最後に配置する TLS/SSL ルール 4 第2章 推奨ポリシーとルールの設定 7 推奨ポリシーとルールの設定 7 SSL ポリシー の設定 8 アクセス コントロール ポリシーの設定 9 第3章 TLS/SSL ルール 例 11 TLS/SSL ルール 例 11 プレフィルタするトラフィック 11 最初のTLS/SSL ルール:特定のトラフィックを復号しない 12 次の TLS/SSL ルール:特定のテストトラフィックを復号する 13 低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない 14

カテゴリの [復号-再署名 (Decrypt - Resign)] ルールの作成 15

最後の TLS/SSL ルール:証明書とプロトコルバージョンをブロックまたは監視する 17

例:証明書ステータスを監視またはブロックする TLS/SSL ルール 18

例:プロトコルバージョンを監視またはブロックする TLS/SSL ルール 21
 オプションの例:証明書の識別名を監視またはブロックする TLS/SSL ルール 22
 TLS/SSL ルール の設定 24

I

I

【注意】シスコ製品をご使用になる前に、安全上の注意(www.cisco.com/jp/go/safety_warning/)をご確認ください。本書は、米国シスコ発行ド キュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更され ている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照くだ さい。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

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

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

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

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

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

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

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

© 2022 Cisco Systems, Inc. All rights reserved.



TLS/SSL ルール ベスト プラクティス

- TLS/SSL ルール ベスト プラクティス (1ページ)
- ・プレフィルタとフローオフロードによる検査のバイパス (2ページ)
- •[復号しない(Do Not Decrypt)]のベストプラクティス(3ページ)
- [復号-再署名(Decrypt Resign)] と [復号-既知のキー(Decrypt Known Key)] のベスト プラクティス (4 ページ)
- 最初に配置する TLS/SSL ルール (4 ページ)
- 最後に配置する TLS/SSL ルール (4 ページ)

TLS/SSL ルール ベスト プラクティス

この章では、TLS/SSL ルールを持つ SSL ポリシーの例を示し、シスコのベストプラクティス と推奨事項について説明します。まず、SSL ポリシーとアクセス コントロール ポリシーの設 定について説明し、次にすべてのルール、および特定の方法でルールを順序付けすることを推 奨する理由について説明します。

以下は、この章で説明する SSL ポリシーです。

SSL Policy Example

Enter Description

Rule	s Trusted CA Certificates	Undecrypta	ble Actions	Advanced Se	ettings									
									+ 4	Add Category	+ Add Rule	् Search I	Rules	×
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action	
Adm	nistrator Rules													
This	category is empty													
Stan	dard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	🕑 Do 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	1 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		- 8

プレフィルタとフローオフロードによる検査のバイパス

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.

Firepower 4100/9300 が使用可能な場合は、大規模なフローオフロードを使用できます。フロー オフロードは、信頼できるトラフィックに検査エンジンをバイパスさせてパフォーマンスを向 上させる手法です。たとえば、データセンターでサーバーのバックアップを転送するために使 用できます。

[復号しない(Do Not Decrypt)]のベストプラクティス

トラフィックのロギング

何もログに記録しない[復号しない(Do Not Decrypt)]ルールは、管理対象デバイスでの処理 に時間がかかるため、作成しないことを推奨します。いずれかの TLS/SSL ルールタイプを設 定する場合は、ロギングを有効にして、一致するトラフィックを確認できるようにします。

復号できないトラフィックのガイドライン

Web サイト自体が復号できない、または Web サイトで SSL ピン留めが使用されている場合、 特定のトラフィックを復号できないと判断できます。SSL ピン留めでは、ブラウザにエラーが 表示されることなく、復号されたサイトへのユーザーアクセスが効果的に阻止されます。

そのようなサイトのリストは次のように管理されています。

- ・Cisco-Undecryptable-Sites という名前の識別名(DN)グループ
- ・ピン留めされた証明書のアプリケーションフィルタ

トラフィックを復号しており、ユーザーが復号されたサイトにアクセスしたときにブラウザに エラーが表示されないようにする場合は、TLS/SSL ルールの下部に[復号しない(Do Not Decrypt)]ルールを設定することを推奨します。

ピン留めされた証明書のアプリケーションフィルタの設定例を次に示します。

Name		Insert						
DND rule for pinned sites	Enabled	into Category	*	Standard R	Rules	•		
Action								
📀 Do not decrypt 🔹								
Zones Networks VLAN Tags	Users a	Applications Ports	Category Certi	icate DN	Cert Status	Cipher Suite	Version	,
Application Filters C Clear A	II Filters X Av	ailable Applications (40)	c			Selected Applic	cations and Filters (0)	
Q pin	XQ	Search by name				any		_
 Risks (Any Selected) 	4	Il apps matching the filte	r i	Add to Ru	lle			
 Business Relevance (Any Selected) A	irbnb	0					
 Types (Any Selected) 	Α	pple Mail	0					
 Categories (Any Selected) 	C	hase	0					
▼ Tags (1 Selected)	C	ropbox	0					
pinned certificate	40 G	mail	0					
	G	oogle	0					
	G	oogle Accounts Authenti	ication 0					

[復号-再署名(Decrypt - Resign)]と[復号-既知のキー (Decrypt - Known Key)]のベストプラクティス

このトピックでは、[復号-再署名(Decrypt - Resign)]と[復号-既知のキー(Decrypt - Known Key)]のベストプラクティスについて説明します。TLS/SSL ルール

[復号-再署名(Decrypt - Resign)]: 証明書のピン留めによるベストプラクティス

ー部のアプリケーションでは、アプリケーション自体に元のサーバー証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。TLS/SSL そのため、[復号-再署名(Decrypt-Resign)]アクションでTLS/SSL ルールを設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSLのピン留めは中間者攻撃を避けるために使用されるため、防止または回避する方法は ありません。次の選択肢があります。

- そのアプリケーション用に、[復号-再署名(Decrypt-Resign)]ルールよりも順序が前の、 [復号しない(Do Not Decrypt)]ルールを作成します。
- •Web ブラウザを使用してアプリケーションにアクセスするようユーザに指示します。

証明書のピン留めの詳細については、Cisco Secure Firewall Management Center デバイス構成ガ イドの「SSL pinning」セクションを参照してください。

[復号-既知のキー(Decrypt - Known Key)] のベストプラクティス

[復号-既知のキー(Decrypt - Known Key)]ルールアクションは、内部サーバーに向かうトラフィックに使用するアクションなので、ルール([ネットワーク(Networks)]ルール条件)には宛先ネットワークを常に追加する必要があります。その結果、サーバーが配置されているネットワークにトラフィックが直接送信され、ネットワーク上のトラフィックが減少します。

最初に配置する TLS/SSL ルール

パケットの最初の部分に一致するルールを最初に配置します。例として、IPアドレスを参照するルール(「ネットワーク(Networks)]ルール条件)があります。

最後に配置する TLS/SSL ルール

次のルール条件を持つルールは最後に配置する必要があります。そのようなルールの場合、シ ステムでトラフィックを長時間検査する必要があるためです。

•アプリケーション

I

- カテゴリ
- •証明書
- 識別名 (DN)
- •証明書ステータス
- •暗号スイート
- バージョン

I



推奨ポリシーとルールの設定

- 推奨ポリシーとルールの設定 (7ページ)
- •SSL ポリシーの設定 (8ページ)
- アクセスコントロールポリシーの設定 (9ページ)

推奨ポリシーとルールの設定

推奨のポリシー設定は次のとおりです。

- •SSLポリシー:
 - ・デフォルトアクションは[復号しない(Do Not Decrypt)]です。
 - ロギングをイネーブルにします。
 - [SSL v2セッション (SSL v2 Session)]と[圧縮されたセッション (Compressed Session)] の両方で、[復号不可のアクション (Undecryptable Actions)]を[ブロック (Block)] に設定します。
 - ・ポリシーの詳細設定でTLS 1.3 復号を有効にします。
- TLS/SSL ルール: [復号しない(Do Not Decrypt)] ルールアクションが使用されるルール を除く、すべてのルールのロギングを有効にします。(これは任意です。復号されていな いトラフィックに関する情報を表示する場合は、そのルールのロギングも有効にします。)
- •アクセス コントロール ポリシー:
 - SSL ポリシー をアクセス コントロール ポリシーに関連付けます(関連付けをしない と、SSL ポリシーとルールは機能しません)。
 - デフォルトのポリシーアクションを[侵入防御:バランスの取れたセキュリティと接続 (Intrusion Prevention: Balanced Security and Connectivity)]に設定します。
 - ロギングをイネーブルにします。

関連トピック

```
SSL ポリシー の設定 (8 ページ)
TLS/SSL ルール の設定 (24 ページ)
アクセス コントロール ポリシーの設定 (9 ページ)
```

SSL ポリシー の設定

SSL ポリシーに推奨される次のベストプラクティス設定の設定方法。

- ・デフォルトアクションは[復号しない(Do Not Decrypt)]です。
- ロギングをイネーブルにします。
- [SSL v2セッション (SSL v2 Session)] と [圧縮されたセッション (Compressed Session)] の両方で、[復号不可のアクション (Undecryptable Actions)]を[ブロック (Block)]に設定します。
- ・ポリシーの詳細設定で TLS 1.3 復号を有効にします。
- **ステップ1** まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ2 [ポリシー (Policies)]>[アクセスコントロール (Access Control)]>[SSL] をクリックします。
- **ステップ3** SSL ポリシー の横にある [編集(Edit)] (▲) をクリックします。
- ステップ4 ページの下部にある [デフォルトのアクション(Default Action)] リストから、[復号しない(Do Not Decrypt)] をクリックします。 次の図は例を示しています。

Default Action

Do not decrypt

- **ステップ5** 行の最後で、[ロギング(Logging)] () をクリックします。
- ステップ6 [接続の終了時にロギングする(Log at End of Connection)] チェックボックスをオンにします。
- **ステップ7** [OK] をクリックします。
- **ステップ8** [保存 (Save)] をクリックします。
- **ステップ9** [復号不可のアクション(Undecryptable Actions)] タブをクリックします。
- **ステップ10** [SSLv2セッション (SSLv2 Session)]と[圧縮セッション (Compressed Session)]のアクションは[ブロッ ク (Block)]に設定することを推奨します。

ネットワークで SSLv2 を許可しないでください。圧縮された TLS/SSL トラフィックはサポートされてい ないためブロックする必要があります。

各オプションの設定の詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの 「Default Handling Options for Undecryptable Traffic」のセクションを参照してください。

次の図は例を示しています。

Rules	Trusted CA Certific	Cates Undecryptable Actions	Advanced Setting
	Decryption Errors	Block	v
	Handshake Errors	Inherit Default Action	•
S	ession not cached	Inherit Default Action	•
Unsupp	oorted Cipher Suite	Inherit Default Action	•
Unk	nown Cipher Suite	Inherit Default Action	•
	SSLv2 Session	Block	•
Co	mpressed Session	Block	·)

- ステップ11 [詳細設定 (Advanced Settings)] タブページをクリックします。
- ステップ12 [TLS 1.3復号の有効化(Enable TLS 1.3 Decryption)] チェックボックスをオンにします。

次に例を示します。



ステップ13 ページの上部にある[保存(Save)]をクリックします。

次のタスク

TLS/SSL ルールの設定 (24 ページ)の説明に従い、TLS/SSL ルールを設定し、各ルールを 設定します。

アクセス コントロール ポリシーの設定

アクセス コントロール ポリシーに推奨される次のベストプラクティス設定の設定方法:

- SSL ポリシー をアクセス コントロール ポリシーに関連付けます(関連付けをしないと、 SSL ポリシーとルールは機能しません)。
- デフォルトのポリシーアクションを[侵入防御:バランスの取れたセキュリティと接続 (Intrusion Prevention: Balanced Security and Connectivity)]に設定します。

ロギングをイネーブルにします。

- ステップ1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ2 [ポリシー (Policies)]>[アクセス制御 (Access Control)]をクリックします。
- ステップ3 アクセス コントロール ポリシーの横にある [編集(Edit)] (▲) をクリックします
- ステップ4 (SSL ポリシーがまだ設定されていない場合は、後で設定できます)。
 - a) 次の図に示すように、ページの上部にある[SSLポリシー (SSL Policy)]の横にある[なし (None)]と いう単語をクリックします。

AC Policy			You have unsaved changes	Show Warnings	Analyze Hit Counts	Save Cancel
Enter Description						
Rules Security Intelligence H	TTP Responses Logging	Advanced	Prefilter Policy: Defau	It Prefilter Policy	SSL Policy: None	Policy Assignments (0) Identity Policy: None

b) リストから、有効にする SSL ポリシーの名前をクリックします。次の図は例を示しています。

SSL Policy to use for inspecting encrypted connections	?
SSL Policy Example	
Revert to Defaults Cancel O	k

- c) [OK] をクリックします。
- d) ページの上部にある[保存 (Save)]をクリックします。
- **ステップ5** ページの下部にある [Default Action(デフォルトアクション)] リストで、[侵入防御:バランスの取れたセキュリティと接続(Intrusion Prevention: Balanced Security and Connectivity)] をクリックします。 次の図は例を示しています。

Default	Action

Intrusion Prevention: Balanced Security and Connectivil 🔻 🖃 📋

- **ステップ6** [ロギング (Logging)] (■) をクリックします。
- ステップ7 [接続の終了時にロギングする(Log at End of Connection)] チェックボックスをオンにして、[OK] をクリックします。
- **ステップ8** [保存 (Save)] をクリックします。

次のタスク

TLS/SSL ルール 例 (11 ページ) を参照してください。



TLS/SSL ルール 例

- TLS/SSL ルール 例 (11 ページ)
- プレフィルタするトラフィック (11ページ)
- ・最初の TLS/SSL ルール:特定のトラフィックを復号しない(12ページ)
- •次のTLS/SSL ルール:特定のテストトラフィックを復号する (13ページ)
- ・低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない(14ページ)
- カテゴリの [復号-再署名 (Decrypt Resign)] ルールの作成 (15ページ)
- 最後の TLS/SSL ルール:証明書とプロトコルバージョンをブロックまたは監視する (17 ページ)
- TLS/SSL ルールの設定 (24 ページ)

TLS/SSL ルール 例

この章では、TLS/SSLルールの例を示し、シスコのベストプラクティスについて説明します。

プレフィルタするトラフィック

プレフィルタリングはアクセス制御の最初のフェーズで、よりリソース消費の大きい評価を実 行する前に行われます。プレフィルタリングは、内部ヘッダーを使用した、より堅牢なインス ペクション機能を備えた後続の評価と比較すると、シンプルかつ高速で、初期に実行されま す。

プレフィルタリングは、セキュリティのニーズとトラフィックプロファイルに基づいて検討す る必要があるため、以下を対象とするポリシーとインスペクションから除外する必要がありま す。

- Microsoft Outlook 365 などの一般的な社内アプリケーション
- ・サーバーバックアップなどのエレファントフローhttps://en.wikipedia.org/wiki/Elephant flow

最初の TLS/SSL ルール:特定のトラフィックを復号しない

例の最初のTLS/SSLルールでは、内部ネットワーク(intranet として定義)に向かうトラフィックは復号されません。[復号しない(Do Not Decrypt)]ルールアクションは、ClientHello中に 一致するため、非常に高速に処理されます。

	SSL	Policy Example												Save	Cancel
	Rule	s Trusted CA Certificates	Undecryptable	e Actions	Advanced Sett	ings									
										+ Add	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	
	Admi	nistrator Rules													
	This	category is empty													
-	Stand	lard Rules DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	On 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 Ur	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													
	Defau	ult Action											Do not decrypt		- 8

(注)

内部 DNS サーバーから内部 DNS リゾルバ (Cisco Umbrella 仮想アプライアンスなど) に向か うトラフィックがある場合は、それらのトラフィックにも[復号しない (Do Not Decrypt)]ルー ルを追加できます。内部 DNS サーバーで独自のログが記録される場合、それらをプレフィル タリングポリシーに追加することもできます。

ただし、インターネットルートサーバー(たとえば、Active Directory に組み込まれた Microsoft 内部 DNS リゾルバ)など、インターネットに向かう DNS トラフィックには、[復号しない(Do Not Decrypt)] ルールやプレフィルタリングを使用しないことを強く推奨します。そのような 場合は、トラフィックを完全に検査するか、ブロックすることを検討する必要があります。

ame		Move				
DND internal source network	Enabled	below rule	v 1			
ction						
O not decrypt						
Zones Networks VLAN Tag	gs Users	Applications Ports	Category Certificate DM	V Cert Status	Cipher Suite Version	Loggin
vailable Networks C	+		Source Networks (1)		Destination Networks (0)	
R Search by name or value			Intranet	Ì	any	
Networks Geolocation						
any						
Pv4-Private-All-RFC1918						
any-ipv4						
any-ipv6						
defaultgateway						
nsidesubnet						
ntranet			Enter an IP address	Add	Enter an IP address	Ade
Pv4-Benchmark-Tests						

次の TLS/SSL ルール:特定のテストトラフィックを復号 する

この例では、次のルールはオプションです。このルールは、限られたタイプのトラフィックを 復号および監視してから、ネットワーク上で許可するか判断する場合に使用します。

Ru	les Trusted CA Certificates	Undecrypta	ble 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	ministrator 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	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lo	any	any	any	any	🕑 Do not de
4	Do not decrypt applications	any	any	any	any	ariy	any	Facebook Facebook Mes Facebook Pho	any	any	any	âny/	🕑 Do not de
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U	i 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	ot Rules												



ne								
ecrypt test site Cable	ed <u>Move</u>							
ion								
Decrypt - Resign vith IntCA	V	🕶 C 🔽 R	eplace Key Only	ý				
ones Networks VLAN Tags Users	Applications Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Loggin
egories C	Reputations					Selected Categ	ories (1)	
Search by name or value	Any					Astrology (An	y reputation)	
ny (Except Uncategorized)								
ncategorized								
dult								
dvertisements								
cohol								
nimals and Pets								
ts								
	Apply to unknown	reputation						

低リスクのカテゴリ、レピュテーション、またはアプリ ケーションを復号しない

ネットワーク上のトラフィックを評価して、低リスクのカテゴリ、レピュテーション、または アプリケーションに一致するトラフィックを判断し、[復号しない(Do Not Decrypt)]アクショ ンを使用して、それらのルールを追加します。トラフィックの処理により多くの時間がかかる ため、それらのルールは他のより具体的な[復号しない(Do Not Decrypt)]ルールの後に配置 します。

次に例を示します。

Ru	les Trusted CA Certificates	Undecryptal	ble Actions	Advanced Se	ttings								
-	_								+ A0	d Category	+ Add Rule	Q Search F	Rules
	Name	Source	Dest	Source	Dest	VLAN Tags	Users	Applicati	Source	Dest Ports	Categories	SSL	Action
Ada	ministrator Rules					Tugo							
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 decryp
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	алу	any	any	any	Risks: Very Lov	any	any	any	any	OD not decry
4	Do not decrypt applications	any	any	алу	апу	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	OD not decry
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
Roo	ot Rules												

ルールの詳細:

Do not decrypt two risk Color Do not decrypt two risk	ame					
chan Control decrypt Zones Network VLAN Tags User Applications Ports Category Certificate DN Cert Status Cipher Suite Version Loggin Picture All Filters C. Clear All Filters Available Applications (1433) C. Search by name O Search by name D Sophare Citers C. New 1645 D Sophare Citers C. New 1645 D Sophare Citers C. D Sophare Citers C. D Sophare Citers C. Carcell C. C	Do not decrypt low risk	Enabled	Move			
Op not decrypt • Zones Networks VLAN Tags Users Applications Prits Cert Status Cipher Suite Version Loggin pileation Filters C Clear All Filters Available Applications (1483) C Selected Applications and Filters (1) Filters * Risk (Any Selected) 539 Search by name • Filters Risks/very Low. Low Filters * Wery Hugh 733 1300-Esc • • Filters Risks/very Low. Low • • * Wery Hugh 733 1300-Esc •	ction					
Zone Networks VLAN Tags Users Applications Prits Category Certificate DN Cert Status Cipher Suite Version Loggin Assertch by name	📀 Do not decrypt 🔹 👻					
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Certif						
placaton Filters C Clear All Filters Available Applications (1483) C Selected Applications and Filters (1) Search by name Risks (Any Selected) Wery Low 645 Good Comparison of the filter of the f	Zones Networks VLAN Tags	Users	Applications Ports Category C	Certificate DN Cert Status	Cipher Suite Version L	ogging
Search by name Search by name * Risk (Any Selected) • Very Low 181 Internet 181 Internet 181 Internet 181 Internet 181 Internet 180 - Flowers 1000mercis 123Movies 123Movies 126 com 17173.com Internet Internet Internet Internet Internet Risks/Very Low, Low Internet Internet Internet Internet Internet Risks/Very Low, Low Internet </td <td>plication Filters C Clear A</td> <td>II Filters</td> <td>vailable Applications (1483) C</td> <td></td> <td>Selected Applications and Filters (1)</td> <td></td>	plication Filters C Clear A	II Filters	vailable Applications (1483) C		Selected Applications and Filters (1)	
 Risks (Any Selected) Boplus Add to Rule Risks (Very Low, Low It Internet 1-800-Flowers 1-800-Flowers 1-800-Flowers 1-2306.cn 1236.cn 1236.	२ Search by name		Q. Search by name		Filters	
I Very Low 538 I is I Internet I is	 Risks (Any Selected) 		050plus	Add to Rule	Risks:Very Low, Low	Ξį.
I cow 454 I cow 454 I cow 454 I cow 454 I com 222 I tigh 133 I 23Movies 1 24Movies 2 24Movies <td>Very Low</td> <td>538</td> <td>1&1 Internet</td> <td></td> <td></td> <td></td>	Very Low	538	1&1 Internet			
I medium 282 I high 139 Very High 70 Very Low 580 Very Low 580 I 236.cn 1236.cn 1236.cn 1236.cn 1236.cn I 236.cn I 17173.com I (< Viewing I -100 of 1483 >)I	Low	454	1-800-Flowers			
Image: High in 139 1236.cn 123Movies Image: Wery High in 200 70 123Movies 0 Image: Wery Low is 580 128.com 0 0 Image: Wery Low is 580 Image: Wery Low is 580 0 0 Image: Wery Low is 580 Image: Wery Low is 580 0 0 0 Image: Wery Low is 580 Image: Wery Low is 580 Image: Wery Low is 580 0 0 Image: Wery Low is 580 Image: Wery Low is 580<	Medium	282	1000mercis			
 Very High 70 Business Relevance (Any Selected) Very Low 880 123Movies 126 com 11713.com IC < Viewing 1-100 of 1483 > > Cancel Saw dd Rule dd Rule me Insert Do not decrypt applications Enabled Into Category * Standard Rules * Concel Saw Do not decrypt * Zones Networks VLAN Tags Users Applications (0) C Upin X Q faceb X Risks (Any Selected) Risks (Any Selected) Tags (1 S	High	139	12306.cn			
 Business Relevance (Any Selected) 126.com 127.com I Very Low Standard Rules Cancel Standard Rules Cancel Standard Rules Con of decrypt applications Enabled Insert Con of decrypt Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Loggin pilcation Filters (Contected) Risks (Any Selected) Gacebook Hessage Filters Tags (I) Selected) Categories (Any Selected) Categories (Very High	70	123Movies			
Wery Low 580 17173.com Image: Concelling the filter Image: Con	 Business Relevance (Any Selected 	i)	126.com (
Image: International Systematic Sy	Very Low	580	17173.com 🧃	É .		
To Do not decrypt applications Into Category Standard Rules tion Do not decrypt Do not decrypt Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Clipher Suite Version Loggin plication Filters C Clear All Filters X Available Applications (0) C Selected Applications and Filters (4) Filters v Risks (Any Selected) Q. faceb X Filters Tags: pinned certificate Filter: "faceb" Applications v Risks (Any Selected) Categories (Any Selected) All apps matching the filter Add to Rule Filters v Tags (1 Selected) Categories (Any Selected) Facebook Facebook Facebook v pinned certificate 0 Interview Interview Facebook Facebook v pinned certificate 0 Interview Interview Interview Facebook Facebook v pinned certificate 0 Interview Interview Interview Interview Interview <th>dd Rule</th> <th></th> <th></th> <th></th> <th>Cancel</th> <th>Sav</th>	dd Rule				Cancel	Sav
tion To not decrypt To not d	dd Rule		Insert		Cancel	Save
Ob not decrypt • Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Loggin oplication Filters C Clear All Filters X Available Applications (0) C Selected Applications and Filters (4) Filters R pinn (0, faceb X Add to Rule Filters Tags:pinned certificate Filter."faceb." * Risks (Any Selected) • All apps matching the filter Add to Rule Facebook * Types (Any Selected) • Categories (Any Selected) Facebook Facebook * Tags (1 Selected) • • • Facebook Photos Facebook Photos	dd Rule Ime Do not decrypt applications	Enabled	Insert into Category	Standard Rules	Cancel	Save
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Loggin oplication Filters ° Clear All Filters X Available Applications (0) ° Selected Applications and Filters (4) Selected Applications and Filters (4) Filters Tags:pinned certificate Filter."faceb" Applications v Risks (Any Selected) Q. faceb X Add to Rule Filters Tags:pinned certificate Filter."faceb" Applications v Types (Any Selected) Categories (Any Selected) Add to Rule Facebook Facebook v Tags (1 Selected) T	dd Rule ame Do not decrypt applications	Enabled	Insert into Category	Standard Rules	Cancel	Save
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Clipher Suite Version Loggin pplication Filters () Available Applications (0) () () Selected Applications and Filters (4) Filters Selected Applications and Filters (4) Filters Tags:pinned certificate Available Applications (0) () () Filters Tags:pinned certificate Filters Tags:pinned certificate Filters Tags:pinned certificate Filters	dd Rule ame Do not decrypt applications tition © Do not decrypt	Enabled	Insert into Category	Standard Rules	Cancel	Save
opplication Filters C Clear All Filters X Available Applications (0) C Selected Applications and Filters (4) Q faceb X O, faceb Filters R lisks (Any Selected) Available Applications the filter Add to Rule Business Relevance (Any Selected) All apps matching the filter Add to Rule Y Types (Any Selected) Categories (Any Selected) Filters Y Tags (1 Selected) Facebook Facebook Y pinned certificate 0 Filters	dd Rule ame Do not decrypt applications tion ⊘ Do not decrypt ▼	Z Enabled	Insert into Category	Standard Rules	Cancel	Save
Q. pinn Q. faceb Filters * Risks (Any Selected) Add to Rule Filters * Business Relevance (Any Selected) All apps matching the filter Add to Rule * Types (Any Selected) Categories (Any Selected) Filters * Tags (1 Selected) Filters Selected) * pinned certificate 0	dd Rule ame Do not decrypt applications ction ⊘ Do not decrypt ▼ Zones Networks VLAN Tag:	Enabled :	Insert Into Category Applications Ports Category C		Cancel	Save
 Risks (Any Selected) Business Relevance (Any Selected) Types (Any Selected) Categories (Any Selected) Tags (1 Selected) pinned certificate 0 0 	dd Rule ame Do not decrypt applications ction	Enabled Users Ul Filters X	Insert Into Category Applications Ports Category C	Standard Rules Certificate DN Cert Status	Cipher Suite Version I Selected Applications and Filters (4)	Save
• Rosk (Air) Selected) Applications • Business Relevance (Any Selected) Facebook • Types (Any Selected) Facebook • Tags (1 Selected) Facebook • pinned certificate 0	dd Rule ame Do not decrypt applications ttion	Enabled Users Users	Insert Into Category Applications Ports Category C valiable Applications (0) C Q faceb		Cipher Suite Version I Selected Applications and Filters (4)	Save
v Usubas (cellulation cellulation) Facebook v Types (Any Selected) Facebook Message v Categories (Any Selected) Facebook Photos v Tags (1 Selected) Facebook Photos	dd Rule Do not decrypt applications ettion ⊘ Do not decrypt ▼ Zones Networks VLAN Tag: pplication Filters C Clear / A pplication Filters C Clear / A pplication Filters C Clear / A	Enabled Users Users	Insert Into Category Applications Ports Category C valiable Applications (0) C Q faceb All range matching the films		Cipher Suite Version I Selected Applications and Filters (4) Filters Tags:pined certificate Filter:"faceb"	Save
• (space kit) selected) Facebook Message • Categories (Any Selected) Facebook Photos • Tags (1 Selected) Facebook Photos	dd Rule Do not decrypt applications tion Do not decrypt Cones Networks VLAN Tags pplication Filters C Clear A pinn Risks (Any Selected) Businese Potemane (Any Selected)	Enabled Users Users UFilters X	Insert Into Category Applications Ports Category O vailable Applications (0) C Q faceb All apps matching the filter		Cipher Suite Version II Selected Applications and Filters (4) Filters Tags:pinned certificate Filter:"faceb" Applications	Save .oggin
Categories (Any Selected) Facebook Photos Facebook Photos pinned certificate 0	dd Rule The second seco	Users Users Users JI Filters X	Insert Into Category Applications Ports Category O vailable Applications (0) C Q faceb All apps matching the filter		Cancel Cipher Suite Version Cipher Suite Version Selected Applications and Filters (4) Filters Tags:pinned certificate Filter: "faceb" Applications Facebook	Save
igg (I Selected) planed certificate	dd Rule ame Do not decrypt applications ction Construction Do not decrypt VLAN Tag: polication Filters C Ctear J A pinn Risks (Any Selected) Business Relevance (Any Selected) Types (Any Selected)	Enabled Users Uli Filters X X	Insert Into Category Applications Ports Category O vailable Applications (0) (2 Q faceb All apps matching the filter		Cipher Suite Version I Cipher Suite Version I Selected Applications and Filters Filters Tags:pinned certificate Filter: "faceb" Applications Facebook Facebook Message	Save
printed certaincate U	dd Rule ame Do not decrypt applications tion Do not decrypt ✓ Zones Networks VLAN Tag: pplication Filters C Clear J A pinn ✓ Risks (Any Selected) ✓ Business Relevance (Any Selected) ✓ Types (Any Selected) ✓ Categories (Any Selected) ✓ Categories (Any Selected) ✓ Categories (Any Selected) ✓ Categories (Any Selected)	Enabled Users UI Filters X X J)	Insert Into Category Applications Ports Category O vailable Applications (0) C Q faceb All apps matching the filter		Cipher Suite Version I Selected Applications and Filters (4) Filters Tags:pinned certificate Filter:"faceb" Applications Facebook Facebook Photos	Save
	dd Rule ame Do not decrypt applications tition Do not decrypt Zones Networks VLAN Tagr opplication Filters C Clear A R pinn Risks (Any Selected) Business Relevance (Any Selecter Types (Any Selected) Categories (Any Selected) Categories (Any Selected) Tags (1 Selected)	Enabled Users UlFilters	Insert Into Category Applications Ports Category Covailable Applications (0) C Q faceb All apps matching the filter		Cipher Suite Version I Selected Applications and Filters (4) Filters Tags:pinned certificate Filter:"faceb" Applications Facebook Facebook Message Facebook Photos	Save
	dd Rule ame Do not decrypt applications ction © Do not decrypt	Enabled Users UlFilters	Insert Into Category Applications Ports Category C vailable Applications (0) C Q faceb All apps matching the filter		Cipher Suite Version I Selected Applications and Filters (4) Filters Tags:pinned certificate Filter: "faceb" Applications Facebook Facebook Message Facebook Photos	Save
	dd Rule ame Do not decrypt applications etion © Do not decrypt	C Enabled Users Ul Filters X X d)	Insert into Category Applications Ports Category C vailable Applications (0) (2 Q, faceb All apps matching the filter		Cipher Suite Version II Selected Applications and Filters (4) Filters Tags:pinned certificate Filter: "faceb" Applications Facebook Facebook Message Facebook Photos	Save

カテゴリの[復号-再署名(**Decrypt - Resign**)] ルールの作 成

このトピックでは、未分類のサイトを除くすべてのサイトに対して、[復号-再署名 (Decrypt -Resign)]アクションを使用してTLS/SSL ルール を作成する例を示します。このルールでは、 [キーのみを置換 (Replace Key Only)]オプションを使用します。[復号-再署名 (Decrypt -Resign)]ルールアクションでは常にこのオプションを使用することを推奨します。 [キーのみを置換(Replace Key Only)]オプションを使用すると、自己署名証明書を使用する サイトを参照した場合、Web ブラウザにセキュリティ警告が表示されるため、ユーザーはセ キュリティで保護されていないサイトと通信していることに気付きます。

このルールを最下部に配置することで、両方の長所を活用でき、ルールをポリシーの前に配置 した場合と同じようにパフォーマンスに影響を与えることなく、トラフィックを復号し、必要 に応じて検査できます。

- **ステップ1** まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ2 内部認証局(CA)をSecure Firewall Management Center([オブジェクト(Objects)]>[オブジェクト管理 (Object Management)]、次に[PKI]>[内部CA(Internal CAs)])にアップロードします(まだアップ ロードしていない場合)。
- ステップ3 [ポリシー(Policies)]>[アクセスコントロール(Access Control)]>[SSL] をクリックします。
- **ステップ4** SSL ポリシーの横にある [編集(Edit)] () をクリックします。
- ステップ5 [ルールの追加(Add Rule)]をクリックします。
- ステップ6 [名前(Name)]フィールドにルールを識別する名前を入力します。
- ステップ7 [アクション(Action)]リストから、[復号-再署名(Decrypt Resign)]をクリックします。
- ステップ8 [with] リストから、内部 CA の名前をクリックします。
- **ステップ9** [キーのみを置換(Replace Key Only)] ボックスをオンにします。 次の図は例を示しています。

Name		Insert		
DR rule sample	Enabled	below rule	• 8	
Action				
🚰 Decrypt - Resign 🔻	with IntCA	• C	🔽 Replace Key Only	

- **ステップ10** [カテゴリ (Category)] タブページをクリックします。
- **ステップ11** [カテゴリ(Categories)] リストの上部で、[任意(未分類を除く) (Any (Except Uncategorized))] をク リックします。
- ステップ12 [レピュテーション (Reputations)]リストで、[任意 (Any)]をクリックします。
- **ステップ13** [ルールに追加(Add to Rule)]をクリックします。 次の図は例を示しています。

Editing Rule - Decrypt all except trusted of	t	0
Name Decrypt all except trusted cat ✓ Enabled Action	Move	
Categories ♂ Q. Search by name or value Any (Except Uncategorized) Uncategorized Adult Advertisements Alcohol Animals and Pets Arts Astrology < < Viewing 1-100 of 125 > >	Any Selected Categories (1) Any Any (Except Uncategorized) (Reputations 1 5 - Trusted Any (Except Uncategorized) (Reputations 1 4 - Favorable - Neutral 2 - Questionable - Untrusted 1 - Untrusted - Add to Rule	Ĩ
	Cancel Sav	ve

最後の TLS/SSL ルール:証明書とプロトコルバージョン をブロックまたは監視する

最後の TLS/SSL ルールは、最も具体的で最も処理が必要なルールのため、不正な証明書と安全でないプロトコルバージョンを監視またはブロックするルールです。

									+ A	dd Category	+ Add Rule	Q Search I	₹ules
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Ports	Categories	SSL	Action
Ad	ministrator Rules												
TP	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
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	→ Decryp Resign
3	Do not decrypt low risk	any	any	any	any	any	any/	Risks: Very Lov	any	any	any	any	OD not
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	any	Any (Except U	any	→ Decry 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



例:証明書ステータスを監視またはブロックする TLS/SSL ルール

Editing Rule - Block	k bad ce	ert st	atus									0
Name												
Block bad cert status			Enabled	Move								
Action												
Block		•										
Zones Networks	VLAN	l Tags	Users	Applications Ports	Categor	y (Certificate	DN	Cert Status	Cipher Suite	Version	Logging
Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any					Revert to Defaults
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					

							Cance	el Save
Editing Rule - Block SSL	v3. TLS 1.0							0
Name		Move						
Block SSLv3. TLS 1.0	Enabled	into Category		▼ Standard R	ules	•		
Action								
Block	*							
Zones Networks VL	AN Tags Users	Applications Ports	Category C	Certificate DN	Cert Status	Cipher Suite	Version	Logging
TLS v1.0								
TLS v1.1								
TLS v1.2								
Revert to Defaults								
							Cance	al Save

例:証明書ステータスを監視またはブロックする TLS/SSL ルール

最後の TLS/SSL ルールは、最も具体的で最も処理が必要なルールのため、不正な証明書と安 全でないプロトコルバージョンを監視またはブロックするルールです。このセクションの例 は、証明書のステータスによってトラフィックを監視またはブロックする方法を示していま す。



- (注) [暗号スイート(Cipher Suite)]と[バージョン(Version)]のルール条件は、[ブロック(Block)] または[リセットしてブロック(Block with reset)]のルールアクションが使用されているルー ルでのみ使用します。これらの条件をルールで他のルールアクションとともに使用すると、シ ステムのClientHello処理に干渉し、予測できないパフォーマンスが生じる可能性があります。
- ステップ1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ2 [ポリシー (Policies)]>[アクセスコントロール (Access Control)]>[SSL] をクリックします。
- **ステップ3** SSL ポリシーの横にある [編集(Edit)] (*I*) をクリックします。
- ステップ4 TLS/SSL ルールの横にある [編集(Edit)] (▲) をクリックします。
- ステップ5 [ルールの追加(Add Rule)]をクリックします。
- ステップ6 [ルールの追加(Add Rule)]ダイアログボックスの[名前(Name)]フィールドに、ルールの名前を入力 します。
- ステップ7 [証明書ステータス (Cert Status)]をクリックします。
- **ステップ8** 各証明書ステータスには次のオプションがあります。
 - ・該当する証明書ステータスが存在するときに照合する場合は、[はい(Yes)]をクリックします。
 - •該当する証明書ステータスが存在しないときに照合する場合は、[いいえ(No)]をクリックします。
 - ・ルールが一致するときに条件をスキップする場合は、[任意(Any)]をクリックします。つまり、 [任意(Any)]を選択すると、証明書ステータスの有無に関わらずルールは一致します。
- ステップ9 [アクション(Action)]リストで、[監視(Monitor)]をクリックしてルールに一致するトラフィックの みを監視してログに記録するか、[ブロック(Block)]または[リセットしてブロック(Block with Reset)] をクリックしてトラフィックをブロックし、必要に応じて接続をリセットします。
- ステップ10 ルールへの変更を保存するには、ページの下部にある[保存(Save)]をクリックします。
- ステップ11 ポリシーへの変更を保存するには、ページの上部にある[保存(Save)]をクリックします。

例

組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authorityの発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の1つを失効させたため、システム管理者は Verified Authority から提供された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示していま す。これにより、Verified Authority から発行されたが CRL には登録されておらず、現 状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設 定では、これらの証明書で暗号化されたトラフィックはアクセスコントロールにより 復号および検査されません。



次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化 されたトラフィックと照合し、そのトラフィックをモニターします。

Revoked:	Yes	No	Any
Valid:	Yes	No	Any
Invalid Issuer:	Yes	No	Any
Not Yet Valid:	Yes	No	Any
Invalid CRL:	Yes	No	Any

Self Signed:
Invalid Signature:
Expired:
Invalid Certificate:
Server Mismatch:

d:	Yes	No	Any
re:	Yes	No	Any
d:	Yes	No	Any
te:	Yes	No	Any
:h:	Yes	No	Any

次の例では、無効な発行者の証明書、自己署名された証明書、期限切れの証明書、お よび無効な証明書が着信トラフィックで使用されている場合、トラフィックはこのルー ル条件に一致します。

Revoked:	Yes	No	Any
Valid:	Yes	No	Any
Invalid Issuer:	Yes	No	Any
Not Yet Valid:	Yes	No	Any
Invalid CRL:	Yes	No	Any

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

次の図は、要求のSNIがサーバー名に一致する、またはCRLが有効でない場合に一致 する証明書ステータスのルール条件を示しています。

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

例:プロトコルバージョンを監視またはブロックする TLS/SSL ルール

この例では、TLS 1.0、TLS 1.1、SSLv3 などのセキュアと見なされなくなったネットワーク上のTLSおよびSSLプロトコルをブロックする方法を示します。この例は、プロトコルバージョンルールがどのように機能するかについてもう少し詳細に説明するために含まれています。

非セキュアなプロトコルはすべてエクスプロイト可能なため、ネットワークから除外する必要 があります。この例では、次のようになります。

- SSL ルールの [バージョン (Version)]ページを使用して、一部のプロトコルをブロック することができます。
- SSLv2は復号不可と見なされるため、SSLポリシーの[復号不可のアクション (Undecryptable Actions)]を使用してブロックできます。
- ・同様に、圧縮 TLS/SSL はサポートされていないため、ブロックする必要があります。

(注)

- E) [暗号スイート(Cipher Suite)]と[バージョン(Version)]のルール条件は、[ブロック(Block)] または[リセットしてブロック(Block with reset)]のルールアクションが使用されているルー ルでのみ使用します。これらの条件をルールで他のルールアクションとともに使用すると、シ ステムのClientHello処理に干渉し、予測できないパフォーマンスが生じる可能性があります。
- **ステップ1** まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ2 [ポリシー(Policies)]>[アクセスコントロール(Access Control)]>[SSL] をクリックします。
- **ステップ3 SSL** ポリシーの横にある [編集(Edit)](♪) をクリックします。
- ステップ4 TLS/SSL ルールの横にある [編集(Edit)] (✔) をクリックします。
- ステップ5 [ルールの追加(Add Rule)]をクリックします。
- ステップ6 [ルールの追加(Add Rule)]ダイアログボックスの[名前(Name)]フィールドに、ルールの名前を入力 します。
- **ステップ7** [アクション (Action)]リストから[ブロック (Block)]または[リセットしてブロック (Block with reset)] をクリックします。
- **ステップ8** [バージョン (Version)]ページをクリックします。
- **ステップ9** SSL v3.0、TLS 1.0、TLS 1.1 など、セキュアでなくなったプロトコルのチェックボックスをオンにしま す。引き続きセキュアと見なされているプロトコルのチェックボックスをオフにします。

次の図は例を示しています。

Editing Rule - Block SSLv3. TLS	\$ 1.0									0
Name Block SSLv3. TLS 1.0 Action Block	Enabled	Move								
Zones Networks 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

- ステップ10 必要に応じて他のルール条件を選択します。
- **ステップ11** [保存(Save)] をクリックします。

オプションの例:証明書の識別名を監視またはブロックする TLS/SSL ルール

このルールは、サーバー証明書の識別名に基づいてトラフィックを監視またはブロックする方 法についてのアイデアを提供し、もう少し詳細に説明するために含まれています

識別名は、国コード、共通名、組織、および組織単位で構成できますが、通常は共通名のみで 構成されます。たとえば、https://www.cisco.comの証明書の共通名はcisco.comです。(ただ し、これは必ずしも単純ではありません。一般的な名前を見つける方法については、Cisco Secure Firewall Management Center デバイス構成ガイドの「Distinguished Name Rule Conditions」 セクションを参照してください)。

クライアント要求のURLのホスト名部分は、サーバー名指定(SNI)です。クライアントは、 TLSハンドシェイクのSNI拡張を使用して、接続するホスト名(たとえば、auth.amp.cisco.com) を指定します。次に、サーバーは、単一のIPアドレスですべての証明書をホストしながら、 接続を確立するために必要な、対応する秘密キーと証明書チェーンを選択します。

- ステップ1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ2 [ポリシー (Policies)]>[アクセスコントロール (Access Control)]>[SSL] をクリックします。
- **ステップ3** SSL ポリシーの横にある [編集(Edit)] () をクリックします。
- ステップ4 TLS/SSL ルールの横にある [編集(Edit)] (✔) をクリックします。
- ステップ5 [ルールの追加(Add Rule)]をクリックします。

- ステップ6 [ルールの追加(Add Rule)]ダイアログボックスの[名前(Name)]フィールドに、ルールの名前を入力 します。
- **ステップ7** [アクション (Action)]リストから[ブロック (Block)]または[リセットしてブロック (Block with reset)] をクリックします。
- **ステップ8** [DN] をクリックします。
- **ステップ9** [使用可能な DN(Available DNs)] で、追加する識別名を探します。
 - ・ここで識別名オブジェクトを作成してリストに追加するには(後で条件に追加できます)、[使用可能なDN(Available DNs)]リストの上にある Add(→)をクリックします。
 - 追加する識別名オブジェクトおよびグループを検索するには、[使用可能なDN(Available DNs)]リストの上にある[名前または値で検索(Search by name or value)]プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。
- ステップ10 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択する には、右クリックして[すべて選択 (Select All)]を選択します。
- ステップ11 [サブジェクトに追加(Add to Subject)]または[発行元に追加(Add to Issuer)]をクリックします。

ヒント 選択したオブジェクトをドラッグアンドドロップすることもできます。

- ステップ12 手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。[サブジェクト DN (Subject DNs)]または[発行元 DN (Issuer DNs)]リストの下にある[DN または CN の入力 (Enter DN or CN)]プロンプトをクリックし、共通名または識別名を入力して[追加(Add)]をクリックします。 どちらのリストにも CN または DN を追加できますが、[サブジェクトDN (Subject DNs)]リストに追加 するのが一般的です。
- ステップ13 ルールを追加するか、編集を続けます。
- ステップ14 終了したら、ルールへの変更を保存し、ページの下部にある[保存(Save)]をクリックします。
- ステップ15 ポリシーへの変更を保存するには、ページの上部にある[保存(Save)]をクリックします。

例

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証 明書で暗号化されたトラフィックは許可され、アクセスコントロールにより制御されます。

Subject DNs (1)	I	ssuer DNs (1)	
GoodBakery	Ĩ	CN=goodca.example.com	Ĩ
Enter DN or CN	Add	Enter DN or CN	Add

TLS/SSL ルール の設定

TLS/SSL ルールに推奨されるベストプラクティス設定の設定方法。

TLS/SSL ルール:[復号しない(Do Not Decrypt)]ルールアクションが使用されるルールを除 く、すべてのルールのロギングを有効にします。(これは任意です。復号されていないトラ フィックに関する情報を表示する場合は、そのルールのロギングも有効にします。)

- ステップ1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ2 [ポリシー (Policies)]>[アクセスコントロール (Access Control)]>[SSL] をクリックします。
- **ステップ3** SSL ポリシーの横にある [編集(Edit)] (/) をクリックします。
- **ステップ4** TLS/SSL ルールの横にある [編集(Edit)] (𝗨) をクリックします。
- **ステップ5** [ロギング (Logging)] タブをクリックします。
- ステップ6 [接続の終了時にロギングする (Log at End of Connection)]をクリックします。
- ステップ7 [保存 (Save)]をクリックします。
- ステップ8 ページ最上部にある [保存 (Save)]をクリックします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。