



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 \(1 ページ\)](#)
- [SSL ポリシー の設定 \(2 ページ\)](#)
- [アクセス コントロール ポリシーの設定 \(3 ページ\)](#)

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。
 - ログイ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グイ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、そのルールのログイ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。
 - ログイングをイネーブルにします。

関連トピック

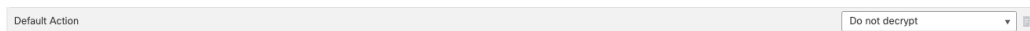
[SSL ポリシー の設定](#) (2 ページ)[TLS/SSL ルール の設定](#)[アクセス コントロール ポリシーの設定](#) (3 ページ)

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。



- 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。

SSL Policy Example
Enter Description

Rules Trusted CA Certificates **Undecryptable Actions** Advanced Settings

Decryption Errors	Block
Handshake Errors	Inherit Default Action
Session not cached	Inherit Default Action
Unsupported Cipher Suite	Inherit Default Action
Unknown Cipher Suite	Inherit Default Action
SSLv2 Session	Block
Compressed Session	Block

Revert to Defaults

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。

Rules Trusted CA Certificates Undecryptable Actions **Advanced Settings**

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

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

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

- Enable TLS 1.3 Decryption

Revert to Defaults

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](#) 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。

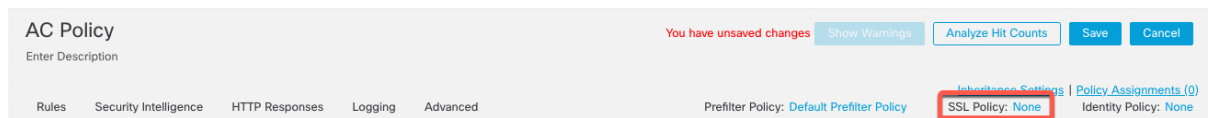
ステップ1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

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。

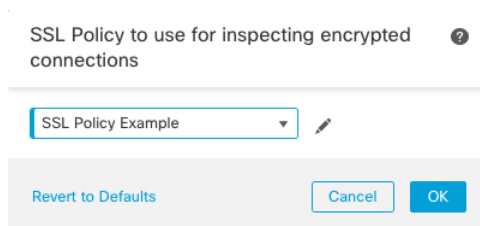
ステップ3 アクセスコントロールポリシーの横にある [編集 (Edit)] (✎) をクリックします

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。

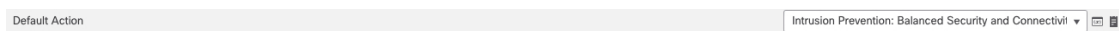


- b) リストから、有効にする SSL ポリシーの名前をクリックします。次の図は例を示しています。



- 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。



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](#) を参照してください。

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。