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

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 （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。

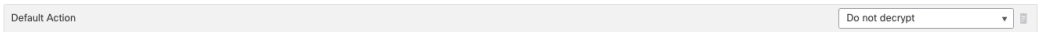
- デフォルトアクションは [復号しない（Do Not Decrypt）] です。
- ロギングをイネーブルにします。
- [SSL v2セッション（SSL v2 Session）] と [圧縮されたセッション（Compressed Session）] の両方で、[復号不可のアクション（Undecryptable Actions）] を [ブロック（Block）] に設定します。
- ポリシーの詳細設定で TLS 1.3 復号を有効にします。

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。

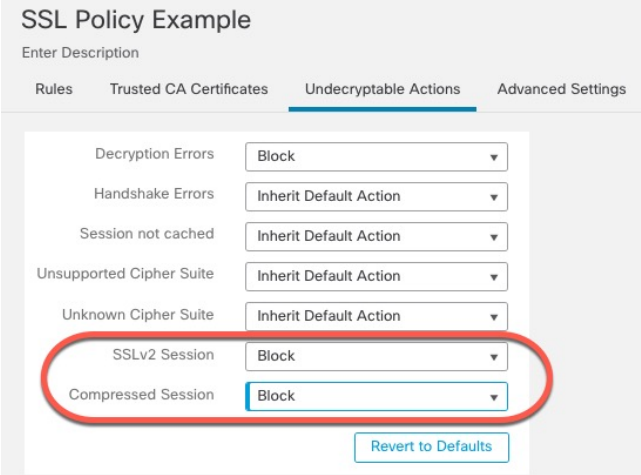
ステップ 9 [復号不可のアクション（Undecryptable Actions）] タブをクリックします。

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。

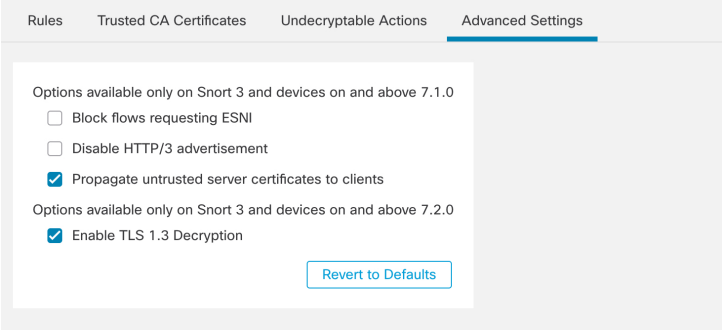
次の図は例を示しています。



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 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。

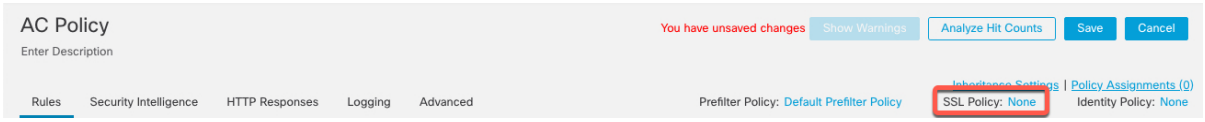
ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

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。

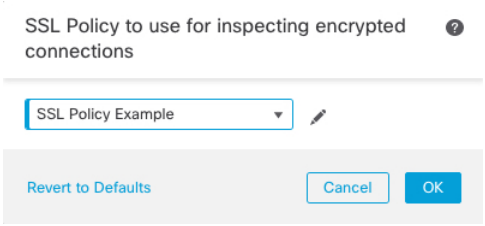
ステップ 3 アクセス コントロール ポリシーの横にある [編集（Edit）]（✎） をクリックします

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。



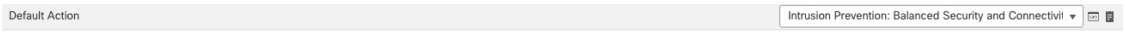
b) リストから、有効にする SSL ポリシーの名前をクリックします。次の図は例を示しています。



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。