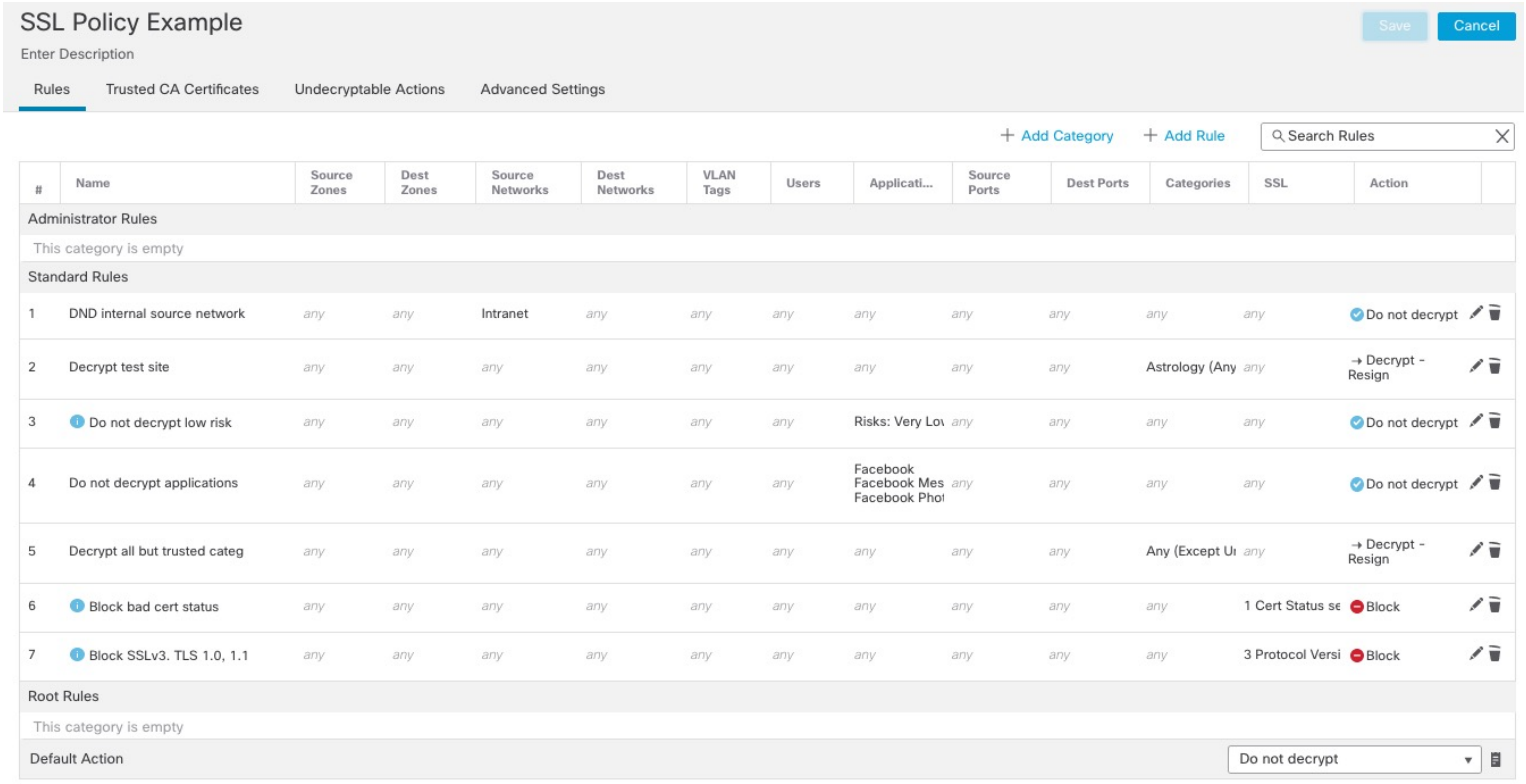
TLS/SSL ルール ベスト プラクティス

TLS/SSL ルール ベスト プラクティス

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。



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

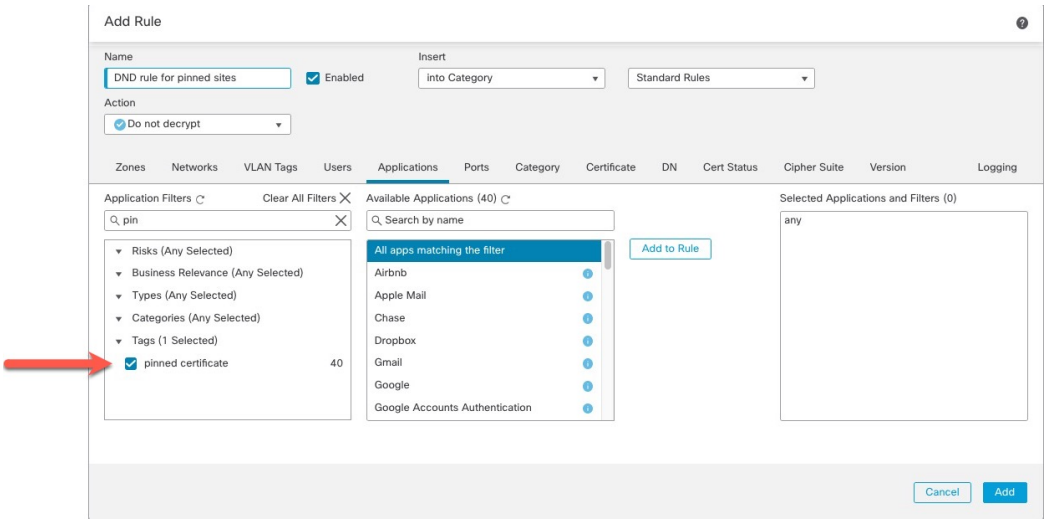
Web サイト自体が復号できない、または Web サイトで SSL ピン留めが使用されている場合、特定のトラフィックを復号できないと判断できます。SSL ピン留めでは、ブラウザにエラーが表示されることなく、復号されたサイトへのユーザーアクセスが効果的に阻止されます。

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。



[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

一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

- 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

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。