# SSL アプライアンスでの基本ルールセットの設定

## 目次



## 概要

ルール セットには、SSL アプライアンスでの SSL トラフィックの処理方法を制御するルールやポリシーが含まれています。 このドキュメントでは、SSL アプライアンスで基本的なルール セットを設定するための手順を示します。

## 従うべき手順

SSL アプライアンスにルール セットを設定するには、次の手順を実行します：

1. [Polices] > [Rulesets] に移動します。

**2.** 新しいルール セットを追加するために緑色のプラス ( + ) 記号を選択します。

3. ルール セットに名前を付け、[OK] を選択します。

**ステップ 4：** 作成したルール セットに新しいルールを挿入するために、[Rules] のセクションからルールの緑色のプラス ( + ) 記号を選択します。 複数のルール セットがある場合は、目的のルール セットの名前をクリックしてから、ルールを追加または変更します。

一般的なルール セットには、以下のルールが含まれています ( ただし、これらに限定されるわけではありません ) 。

1. キーや証明書を入手できる内部 SSL サーバに送信されるトラフィックを、既知のキーや証明書を使用して検査することを指定する 1 つ以上のルール。
2. クライアント証明書を使用する内部サーバがある場会、それらのサーバへのセッションを照合し、トラフィックをカットスルーするための 1 つ以上のルール。
3. クライアント証明書を使用することがわかっている外部サーバ、あるいはトラフィックを検査する必要がない外部サーバがある場合、それらのサーバへのトラフィックをカットスルーする 1 つ以上のルール。
4. そして、一般には、再署名された証明書を使用してすべての SSL セッションを検査するデフォルト アクションも含まれます。

**注:** クライアント証明書を使用するサイトへのトラフィックを検査し、セッションが復号で

きず、セッションが失敗するという可能性は常にあります。 セッション ログは、セッションの詳細と、セッションが終了した理由を示します。これらの詳細は、今後のセッションを成功させるためにどのようにルールを定義すれば良いかを示す十分な情報を提供します。詳細は、『SSL Administration and Deployment Guide』を参照してください。