TLS/SSL ルール 例

- TLS/SSL ルール 例 （1 ページ）
- プレフィルタするトラフィック （1 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 （2 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 （3 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（4 ページ）
- カテゴリの [復号-再署名（Decrypt - Resign）] ルールの作成 （5 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 （7 ページ）
- TLS/SSL ルール の設定 （14 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

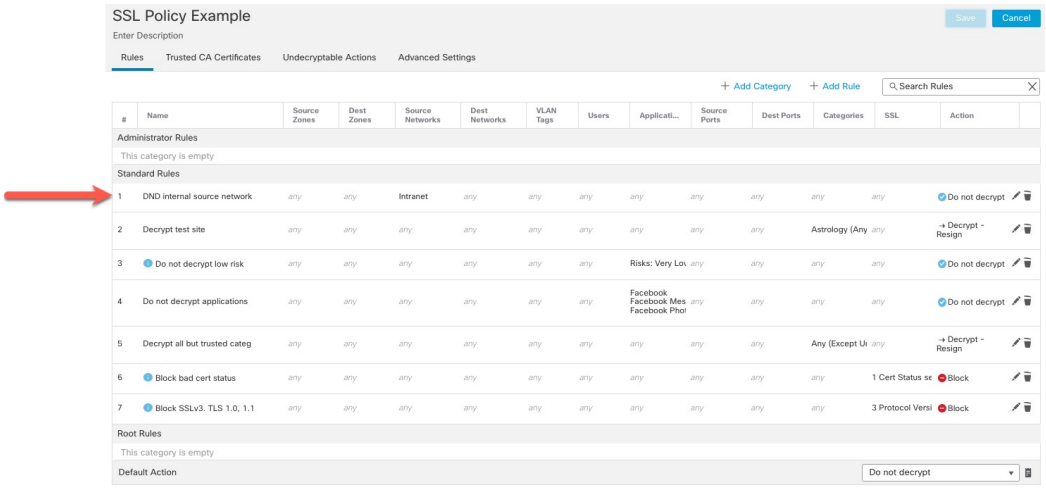
プレフィルタリングはアクセス制御の最初のフェーズで、よりリソース消費の大きい評価を実行する前に行われます。プレフィルタリングは、内部ヘッダーを使用した、より堅牢なインスペクション機能を備えた後続の評価と比較すると、シンプルかつ高速で、初期に実行されます。

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

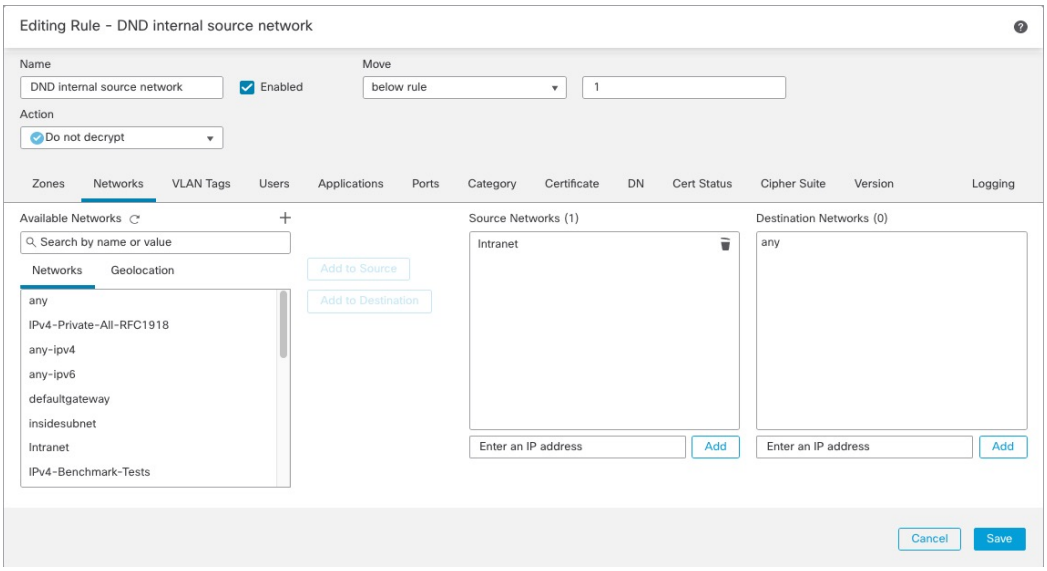
最初の TLS/SSL ルール：特定のトラフィックを復号しない

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。



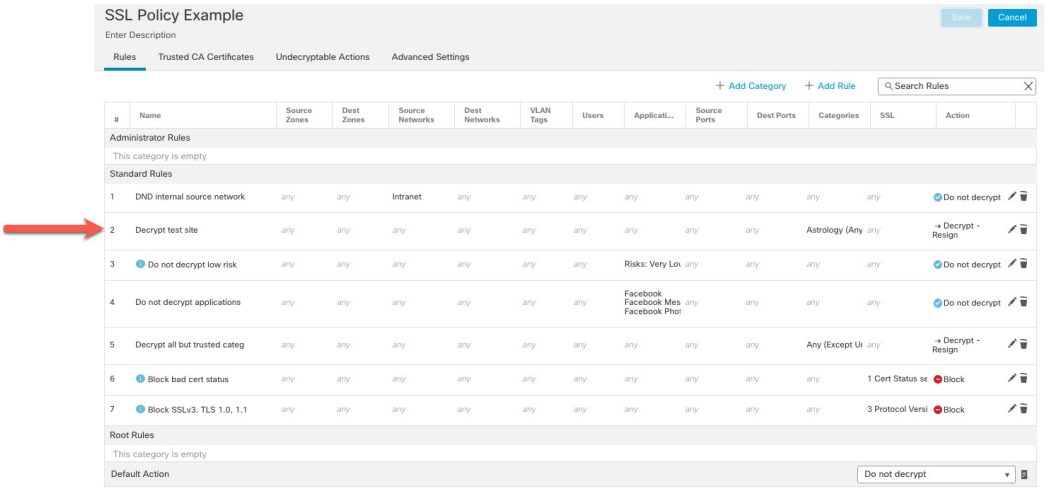
（注） 内部 DNS サーバーから内部 DNS リゾルバ（Cisco Umbrella 仮想アプライアンスなど）に向かうトラフィックがある場合は、それらのトラフィックにも [復号しない（Do Not Decrypt）] ルールを追加できます。内部 DNS サーバーで独自のログが記録される場合、それらをプレフィルタリングポリシーに追加することもできます。

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。

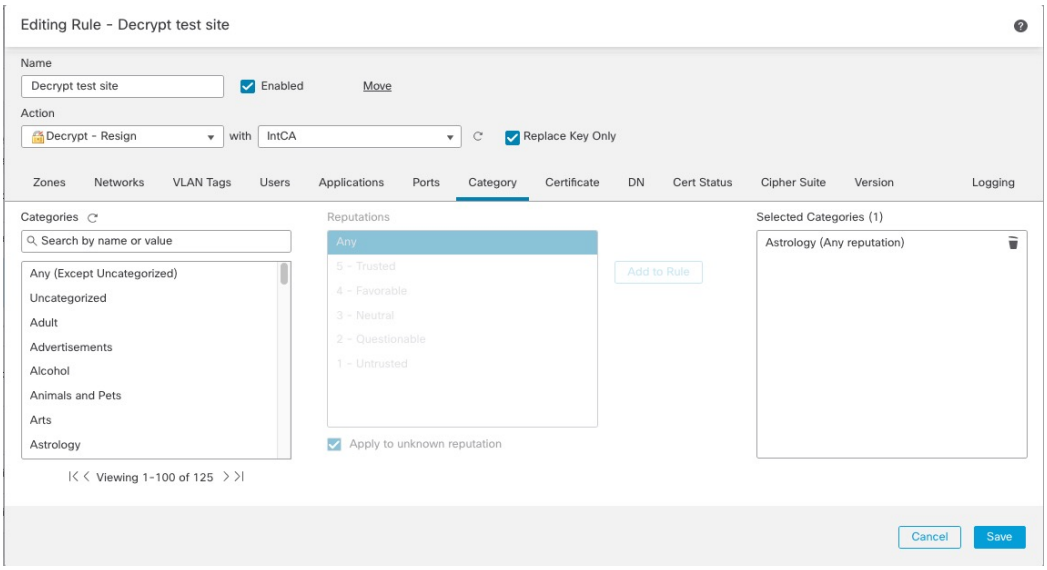


次の TLS/SSL ルール：特定のテストトラフィックを復号する

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。



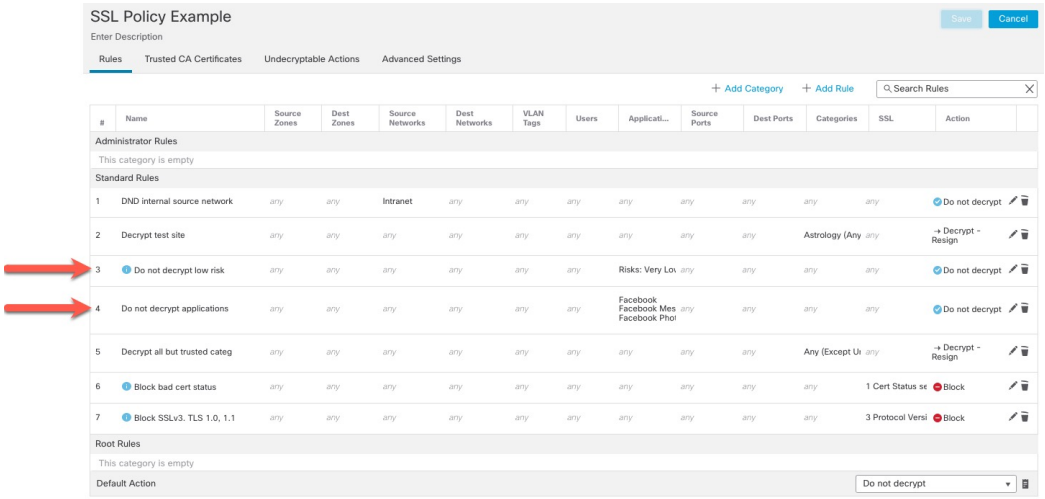
ルールの詳細：



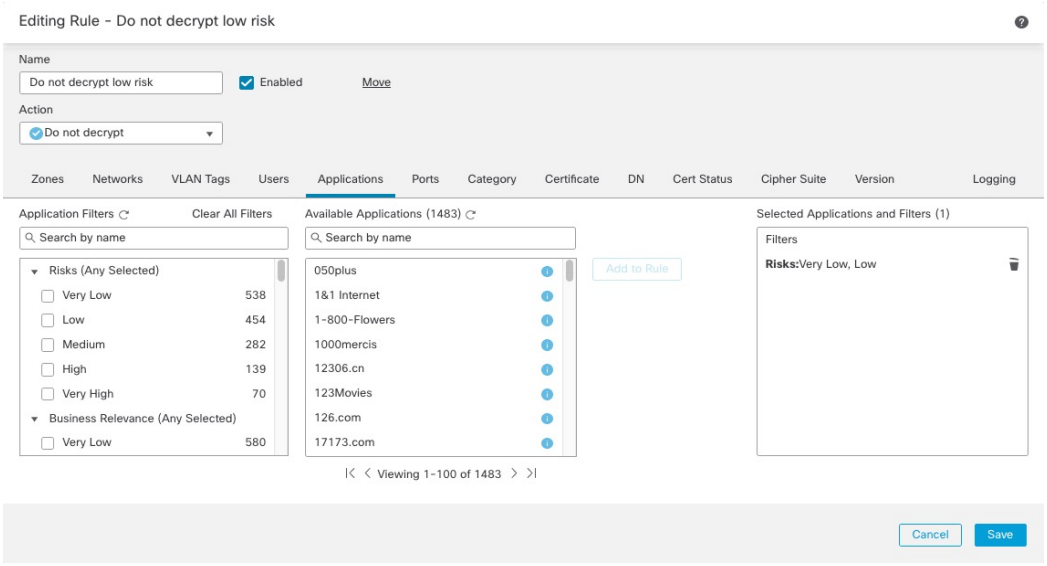
低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない

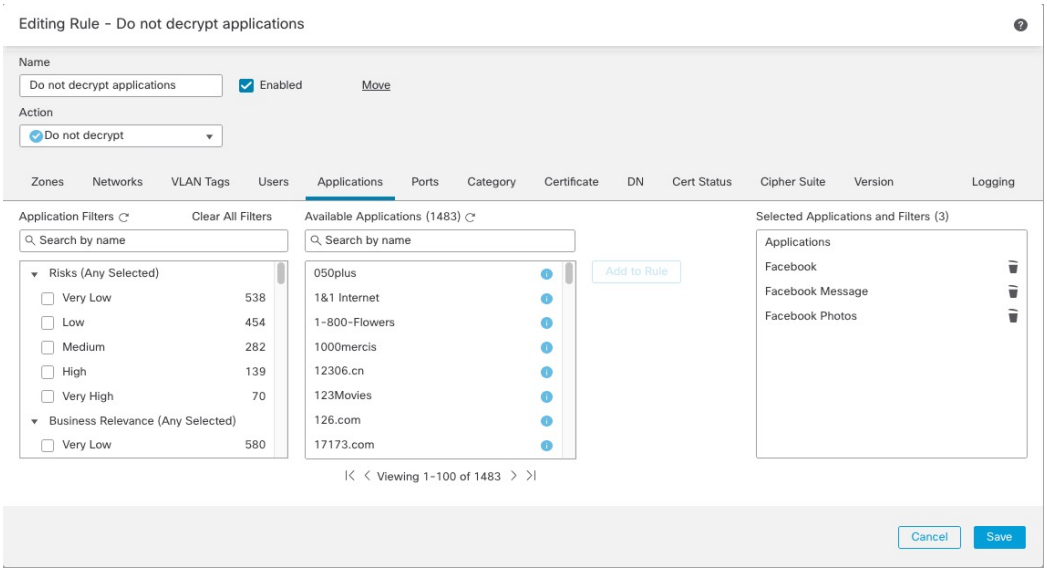
ネットワーク上のトラフィックを評価して、低リスクのカテゴリ、レピュテーション、またはアプリケーションに一致するトラフィックを判断し、[復号しない（Do Not Decrypt）]アクションを使用して、それらのルールを追加します。トラフィックの処理により多くの時間がかかるため、それらのルールは他のより具体的な [復号しない（Do Not Decrypt）] ルールの後に配置します。

次に例を示します。



ルールの詳細：





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。

手順

ステップ 1 まだ Firepower 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 Firepower 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。

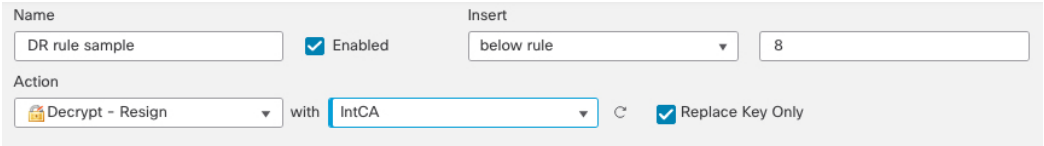
ステップ 6 [名前（Name）] フィールドにルールを識別する名前を入力します。

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。



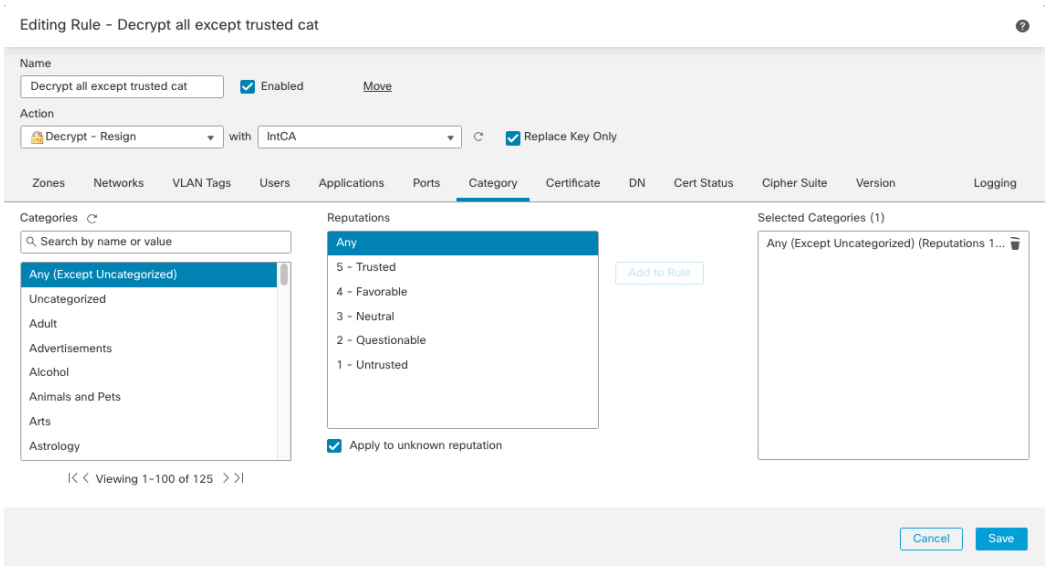
ステップ 10 [カテゴリ（Category）] タブページをクリックします。

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。

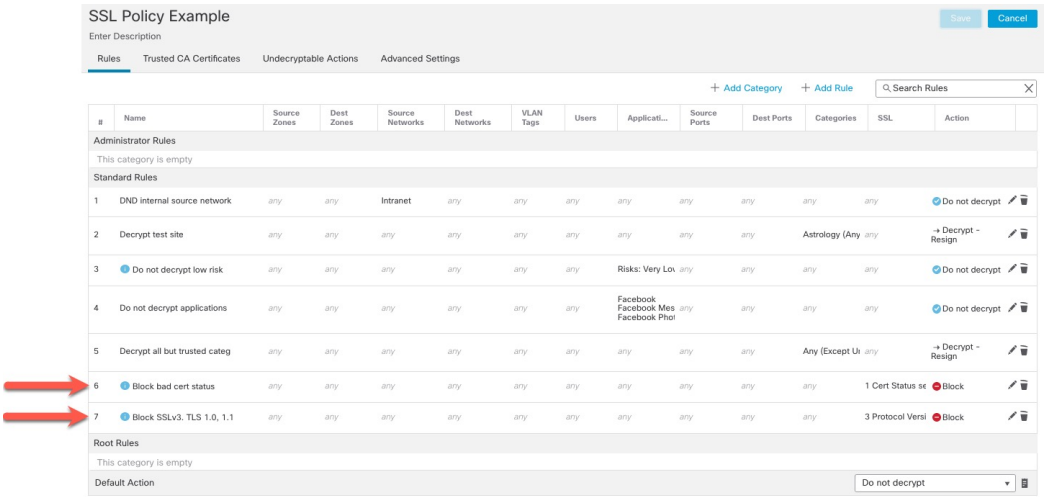
ステップ 13 [ルールに追加（Add to Rule）] をクリックします。

次の図は例を示しています。

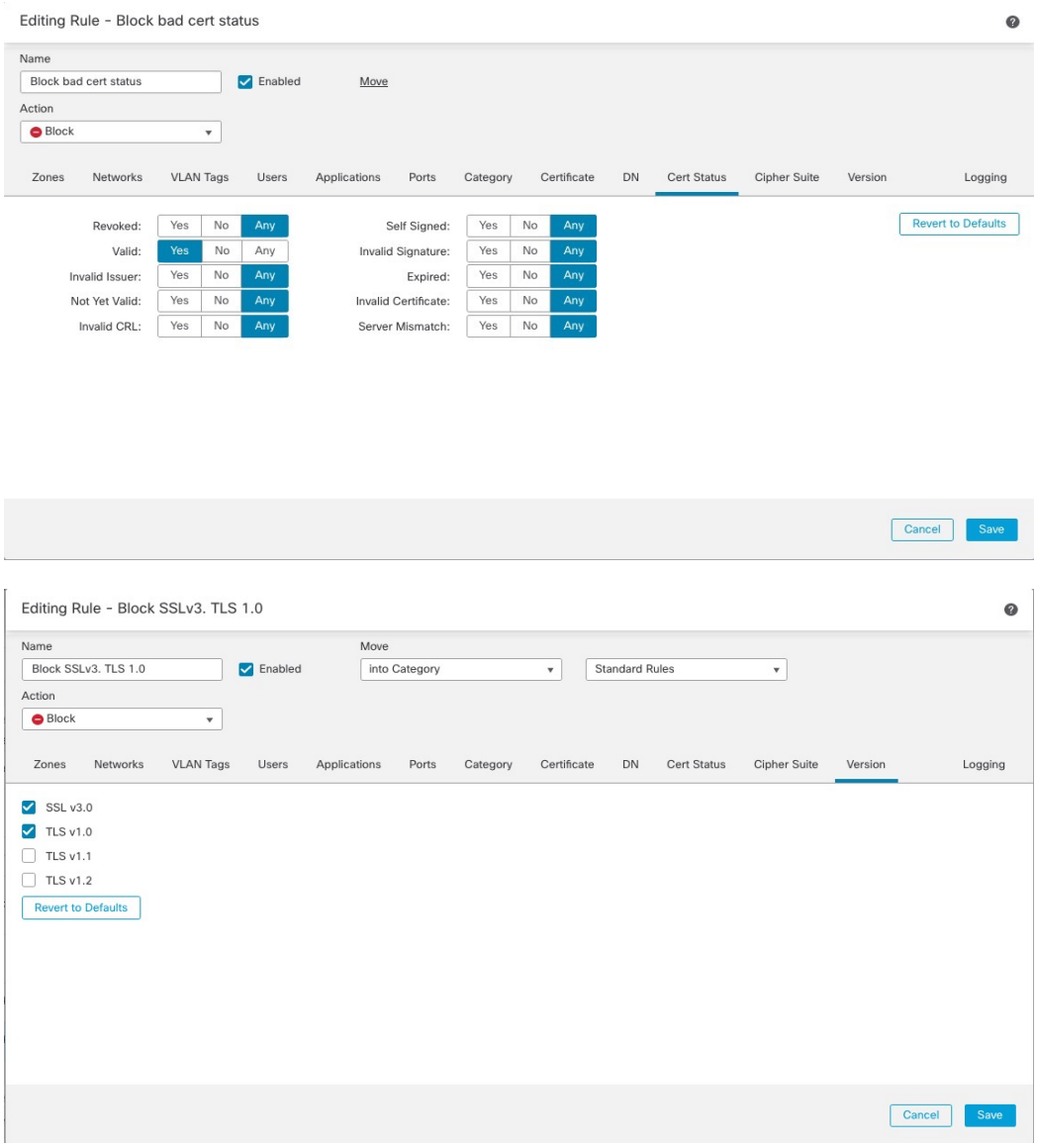


最後の TLS/SSL ルール：証明書とプロトコルバージョンをブロックまたは監視する

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。



ルールの詳細：



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。

手順

ステップ 1 まだ Firepower 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 [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。

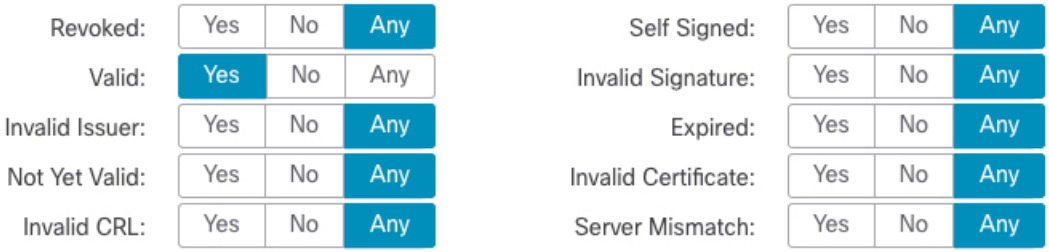
ステップ 11 ポリシーへの変更を保存するには、ページの上部にある [保存（Save）] をクリックします。

例

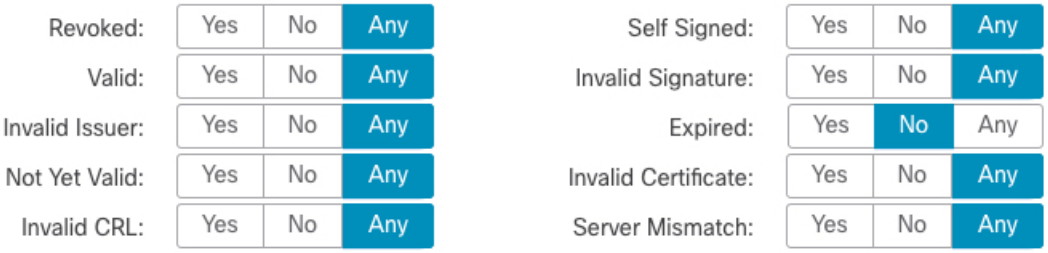
組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から提供された CRL をアップロードします。

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

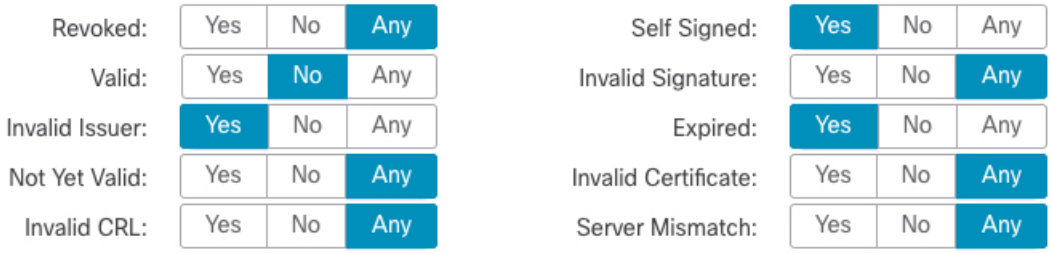
状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。



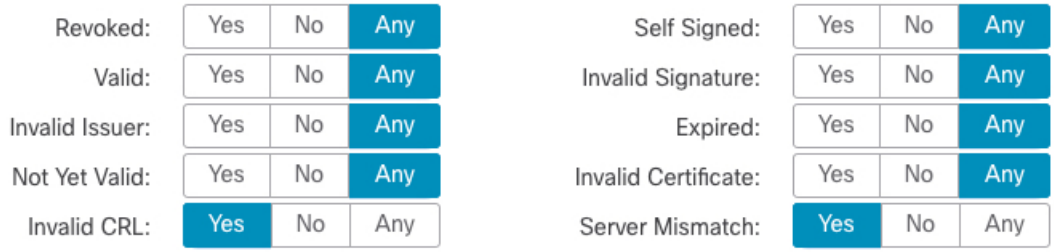
次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合し、そのトラフィックをモニターします。



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。



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。



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） [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。

手順

ステップ 1 まだ Firepower 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。

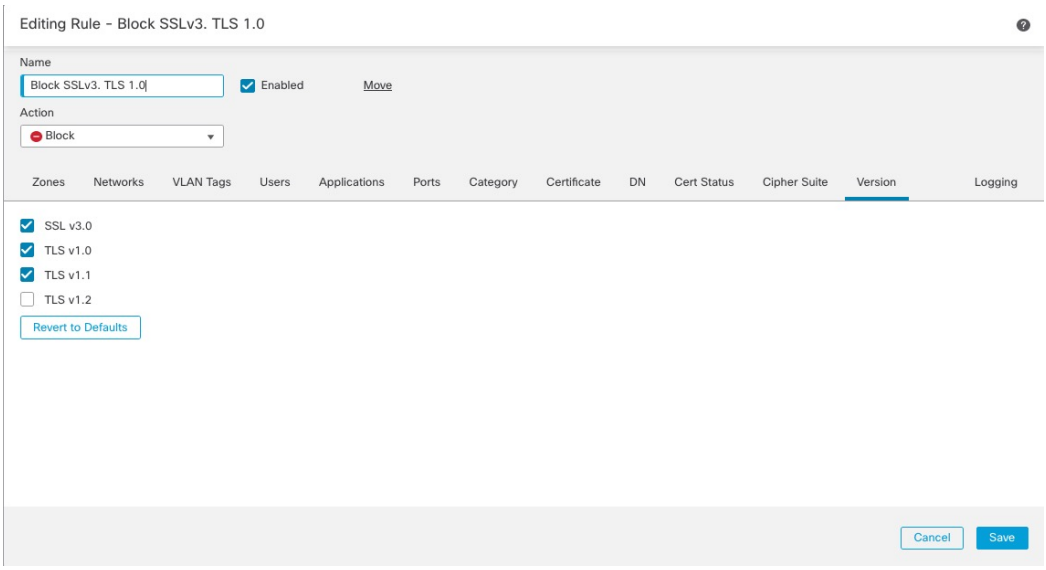
ステップ 6 [ルールの追加（Add Rule）] ダイアログボックスの [名前（Name）] フィールドに、ルールの名前を入力します。

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。



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、Firepower 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。

手順

ステップ 1 まだ Firepower 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。

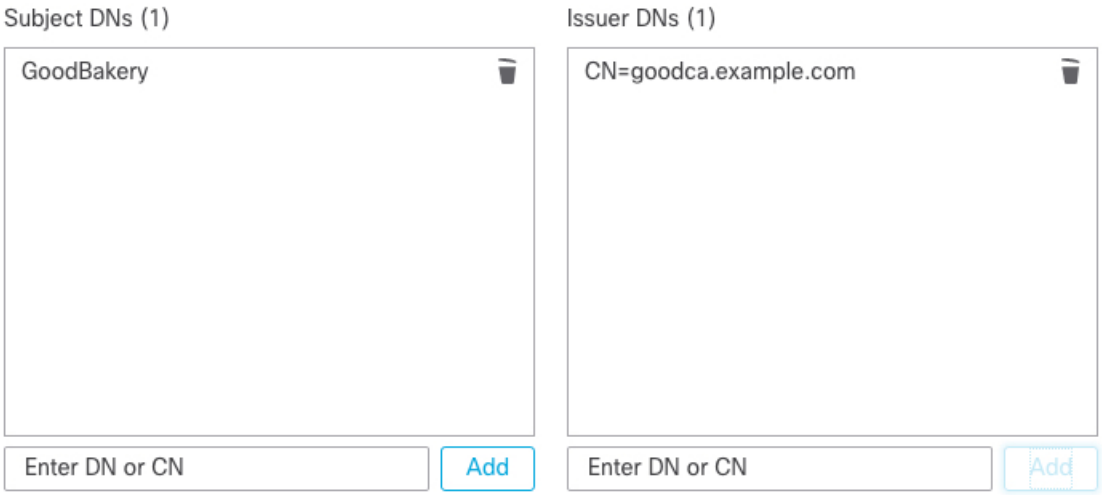
ステップ 13 ルールを追加するか、編集を続けます。

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。



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。）

手順

ステップ 1 まだ Firepower 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 [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。