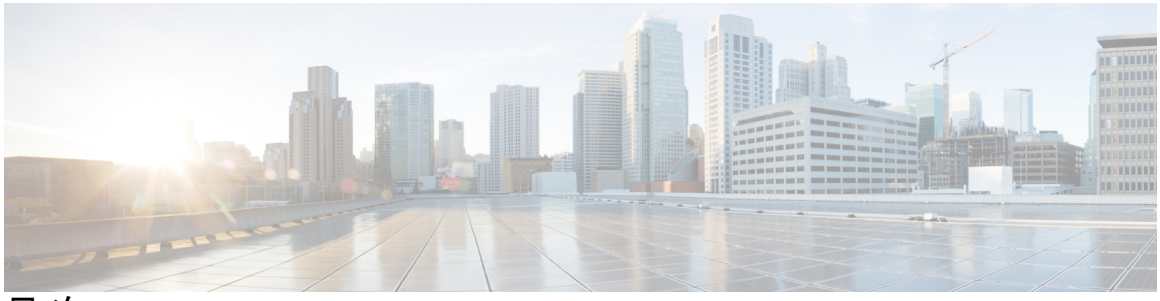
TLS/SSL 7.1 ルールの展開と例

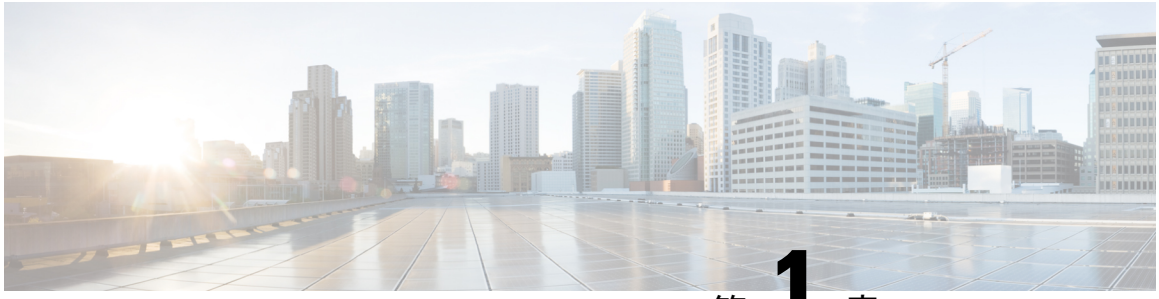
最終更新：2024 年 11 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



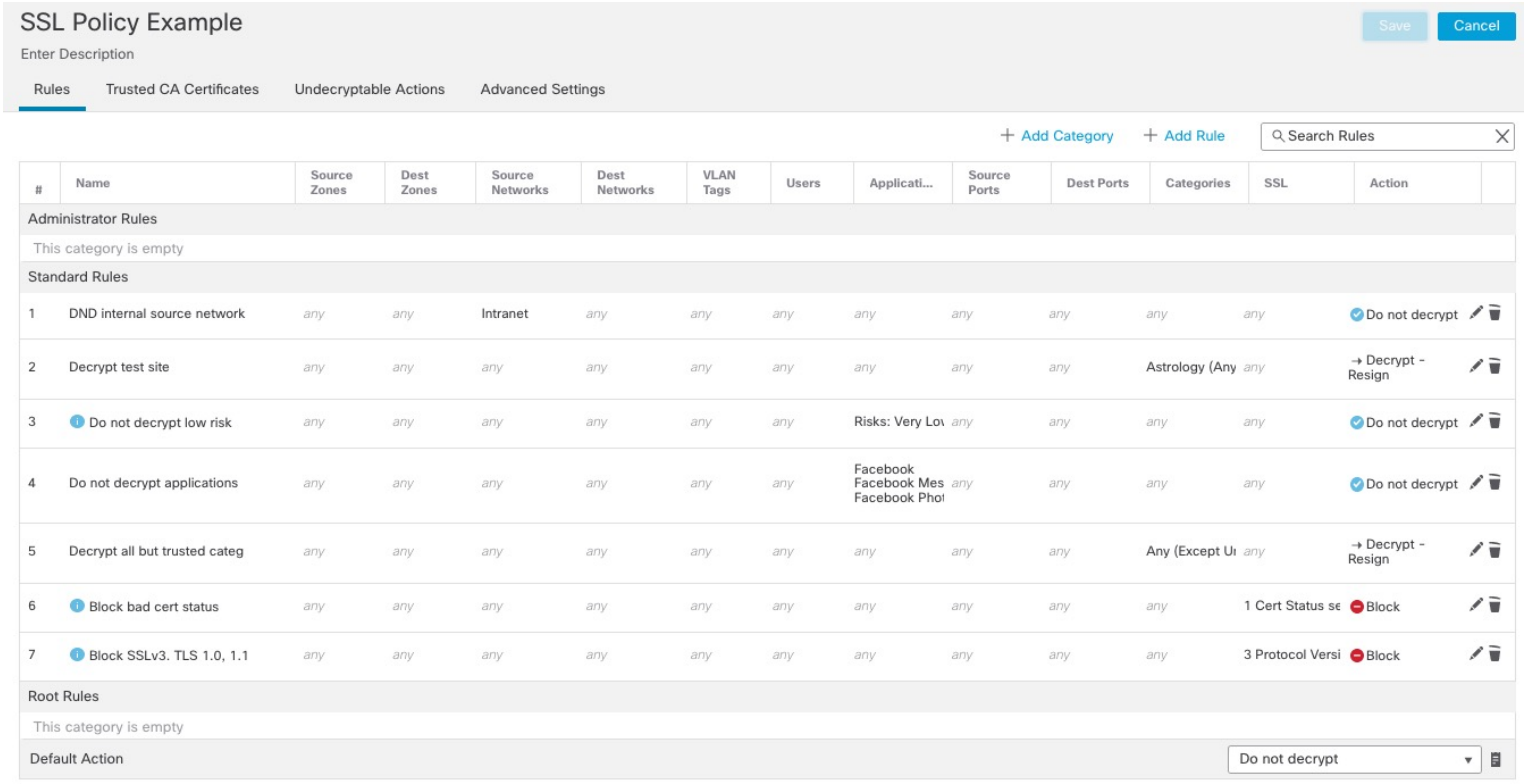
第 1 章

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

プレフィルタはアクセス制御の最初のフェーズで、システムがより大きいリソース消費の評価を実行する前に行われます。プレフィルタリングは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では、限定された外部ヘッダーを基準にしてトラフィックを迅速に処理します。内部ヘッダーを使用し、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このプレフィルタリングを比較します。

次の目的でプレフィルタリングを設定します。

- パフォーマンスの向上：インスペクションを必要としないトラフィックの除外は、早ければ早いほど適切です。特定のタイプのプレーン テキストをファストパスまたはブロックし、カプセル化された接続を検査することなく外側のカプセル化ヘッダーに基づいてトンネルをパススルーします。早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。
- カプセル化トラフィックに合わせたディープインスペクションの調整：同じ検査基準を使用してカプセル化接続を後で処理できるように、特定のタイプのトンネルを再区分できます。アクセス制御はプレフィルタ後に内側のヘッダーを使用するため、再区分は必須です。

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

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。

[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、Firepower 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。

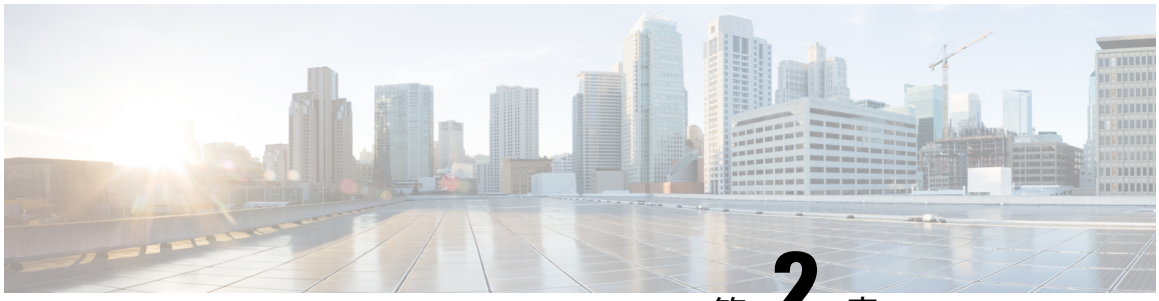
最初に配置する TLS/SSL ルール

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



第 2 章

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。
- 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 （6 ページ）

TLS/SSL ルール の設定 （22 ページ）

アクセス コントロール ポリシーの設定 （7 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。

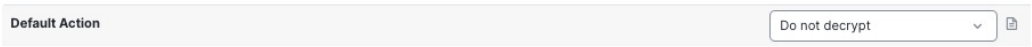
手順

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 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。

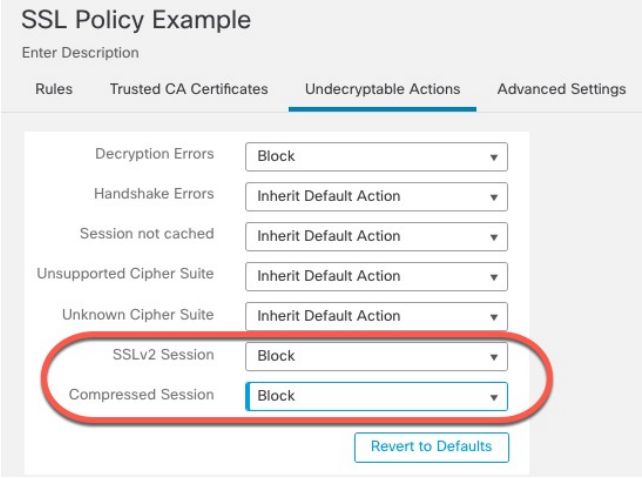
ステップ 9 [復号不可のアクション（Undecryptable Actions）] タブをクリックします。

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、Firepower 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 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　（22 ページ） 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。

手順

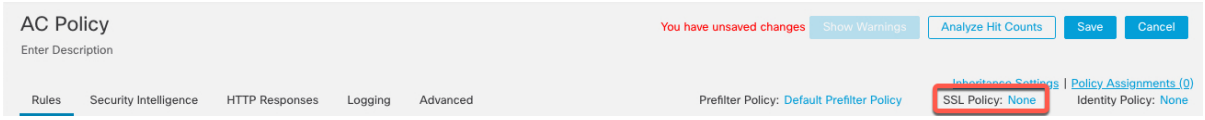
ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

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。

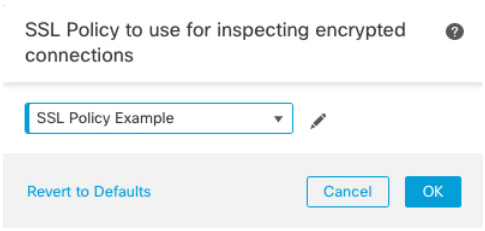
ステップ 3 アクセス コントロール ポリシーの横にある [編集（Edit）]（✎） をクリックします

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。



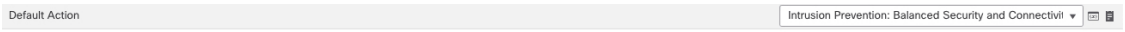
b) リストから、有効にする SSL ポリシーの名前をクリックします。次の図は例を示しています。



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。



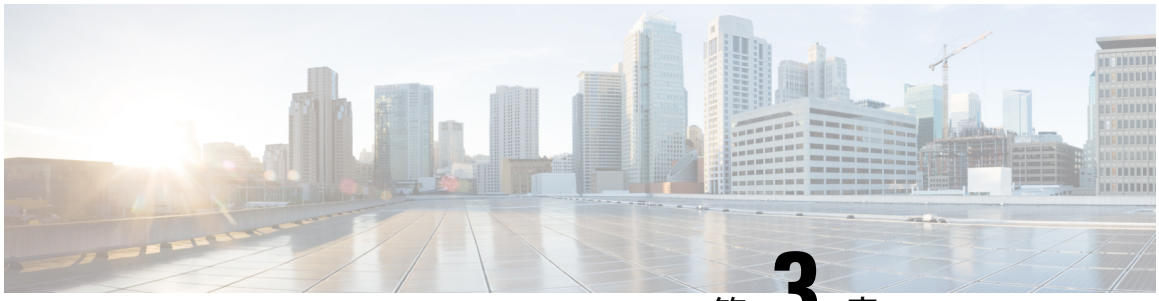
ステップ 6 [ロギング（Logging）]（ ） をクリックします。

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 （9 ページ） を参照してください。



第 3 章

TLS/SSL ルール 例

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

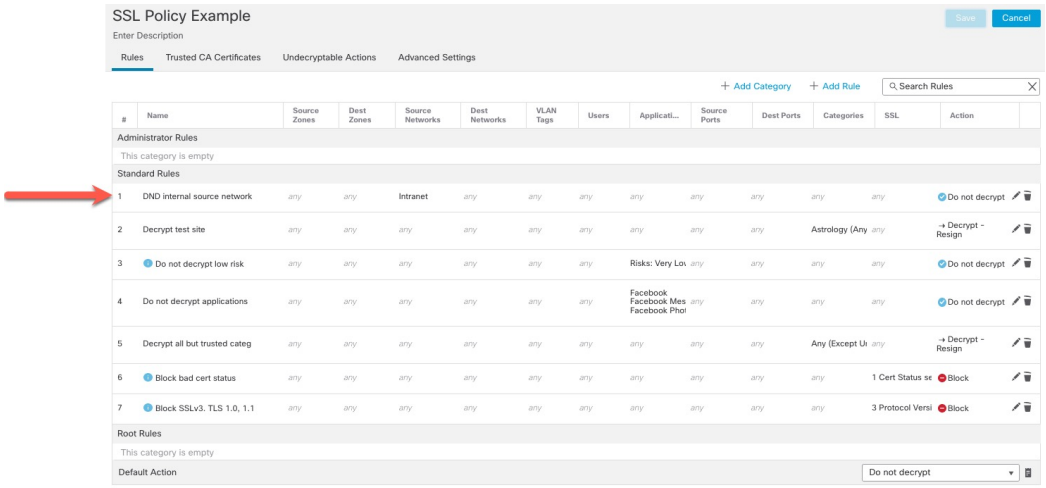
プレフィルタリングはアクセス制御の最初のフェーズで、よりリソース消費の大きい評価を実行する前に行われます。プレフィルタリングは、内部ヘッダーを使用した、より堅牢なインスペクション機能を備えた後続の評価と比較すると、シンプルかつ高速で、初期に実行されます。

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

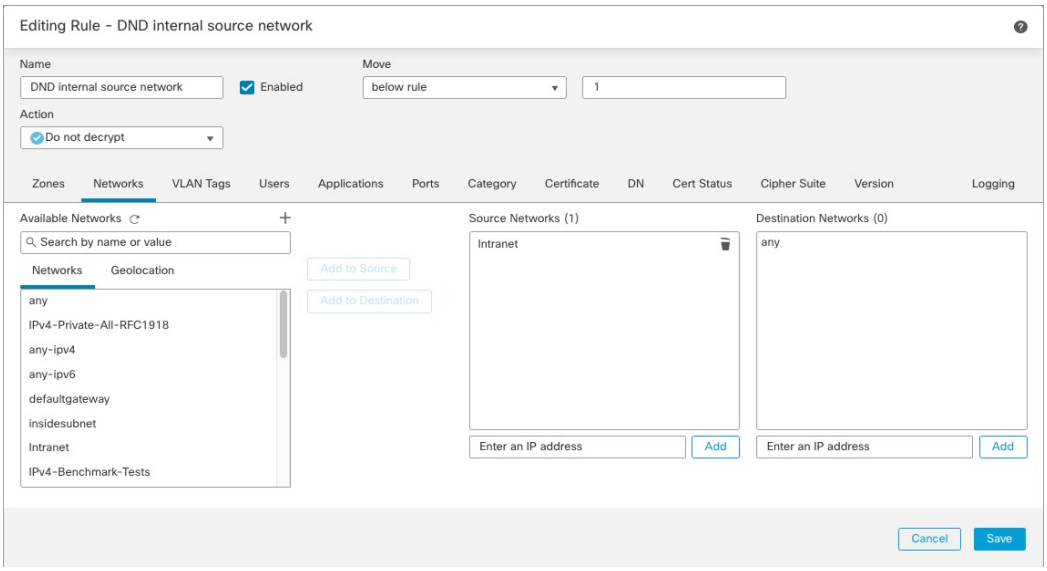
最初の TLS/SSL ルール：特定のトラフィックを復号しない

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。



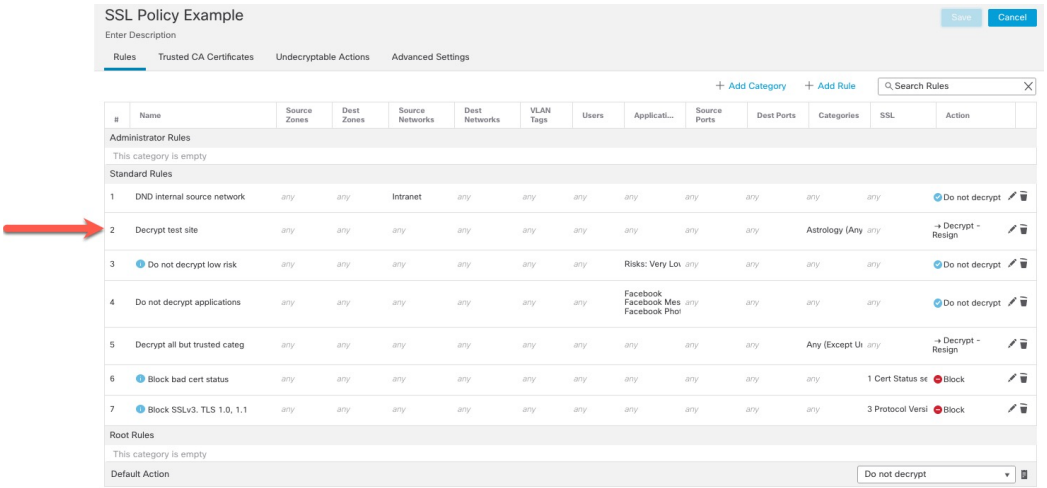
（注） 内部 DNS サーバーから内部 DNS リゾルバ（Cisco Umbrella 仮想アプライアンスなど）に向かうトラフィックがある場合は、それらのトラフィックにも [復号しない（Do Not Decrypt）] ルールを追加できます。内部 DNS サーバーで独自のログが記録される場合、それらをプレフィルタリングポリシーに追加することもできます。

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。

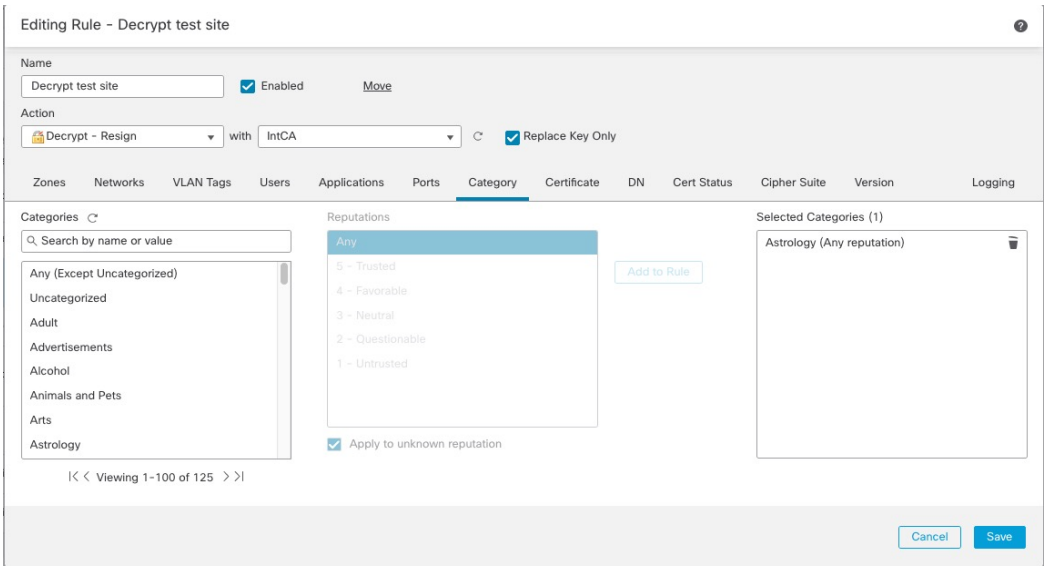


次の TLS/SSL ルール：特定のテストトラフィックを復号する

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。



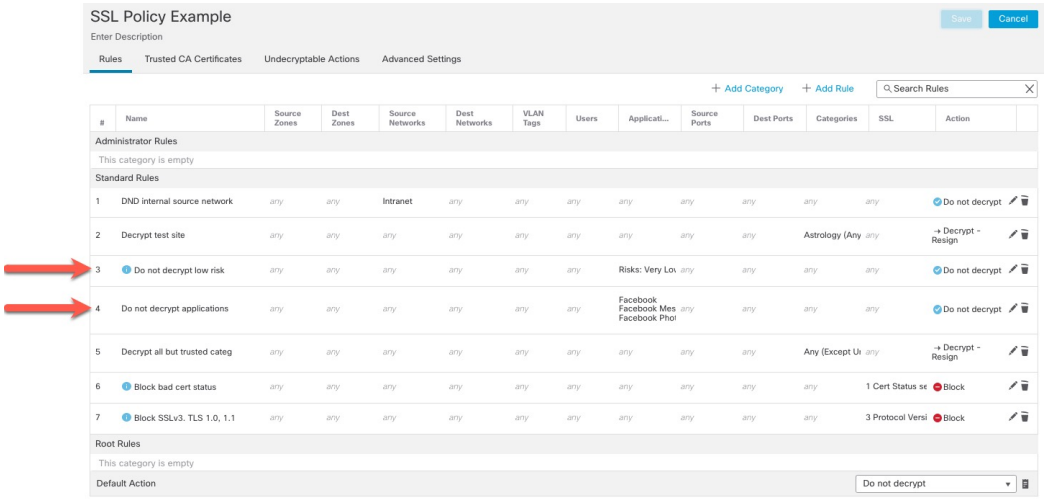
ルールの詳細：



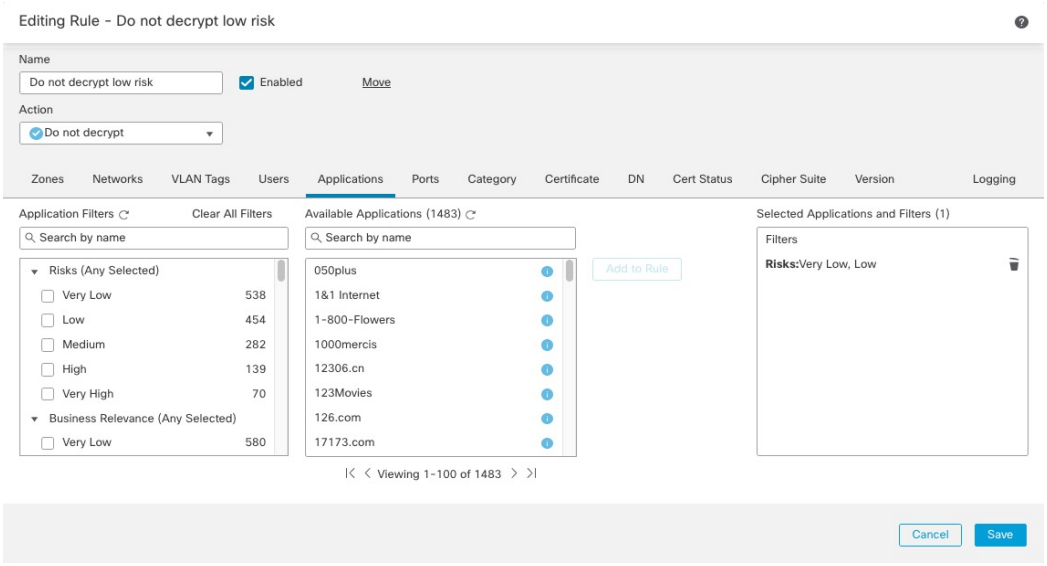
低リスクのカテゴリ、レピュテーション、またはアプリケーションを復号しない

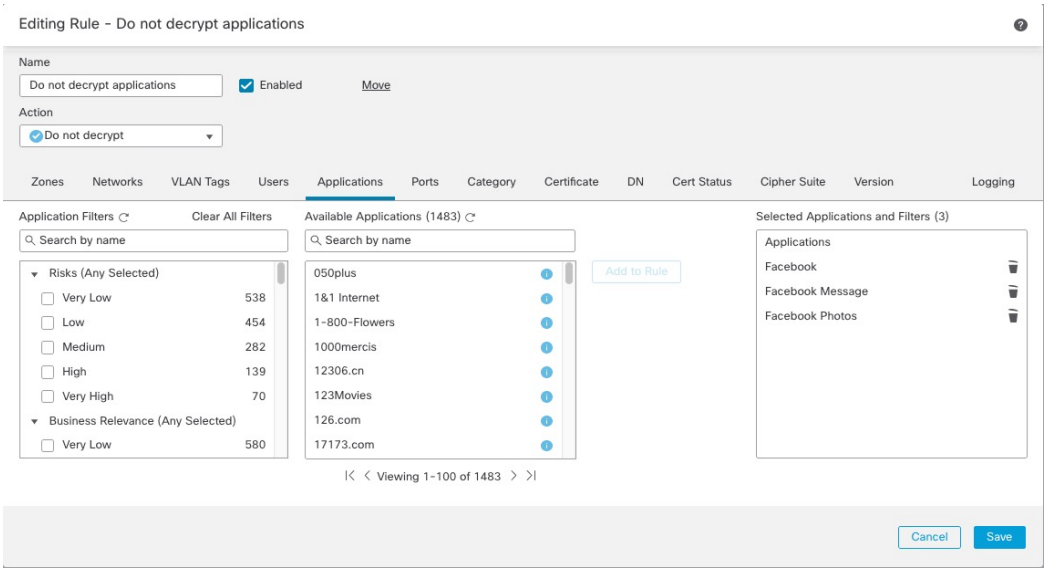
ネットワーク上のトラフィックを評価して、低リスクのカテゴリ、レピュテーション、またはアプリケーションに一致するトラフィックを判断し、[復号しない（Do Not Decrypt）]アクションを使用して、それらのルールを追加します。トラフィックの処理により多くの時間がかかるため、それらのルールは他のより具体的な [復号しない（Do Not Decrypt）] ルールの後に配置します。

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。

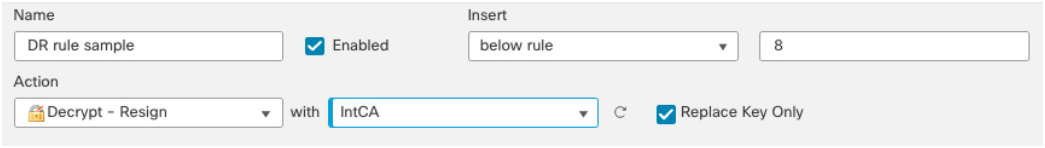
ステップ 6 [名前（Name）] フィールドにルールを識別する名前を入力します。

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。



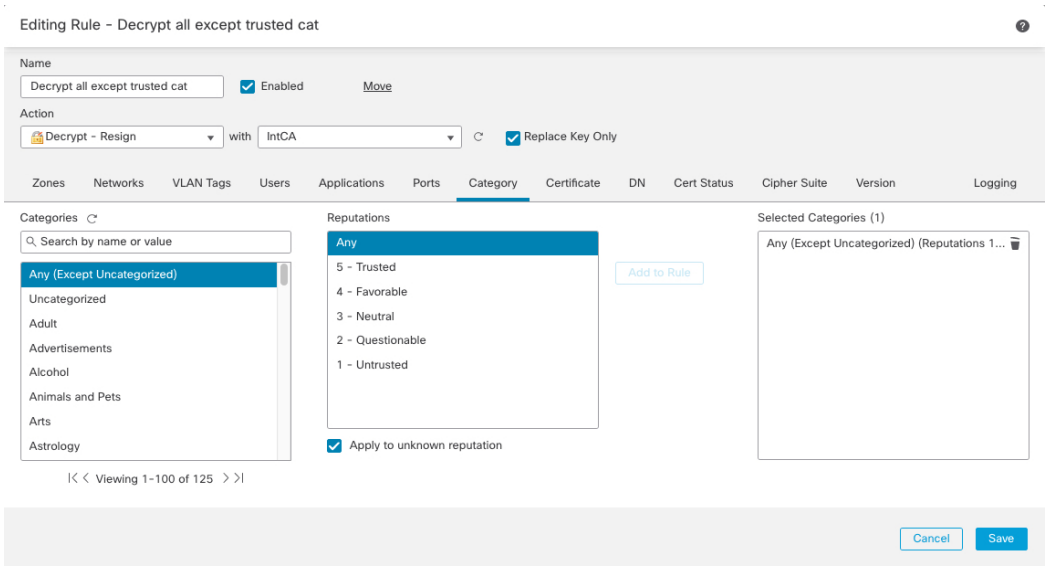
ステップ 10 [カテゴリ（Category）] タブページをクリックします。

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。

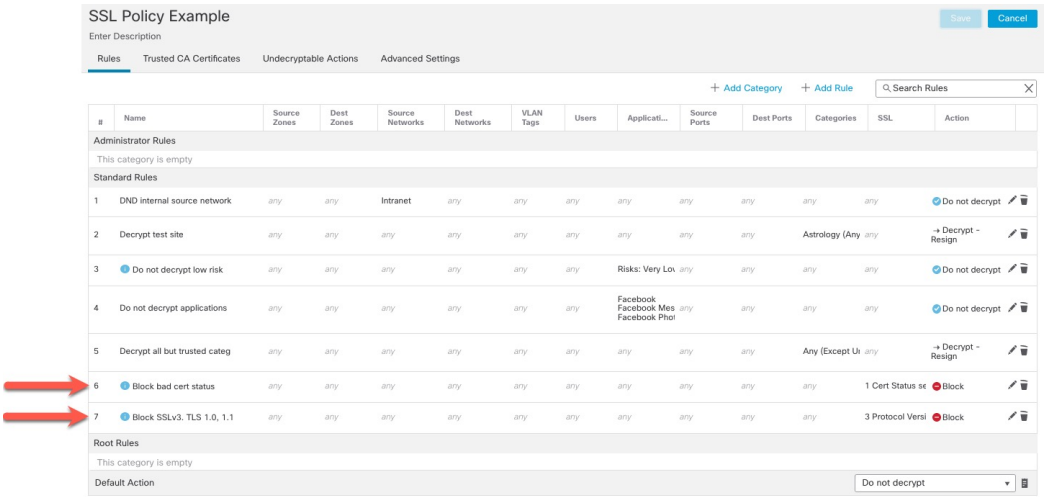
ステップ 13 [ルールに追加（Add to Rule）] をクリックします。

次の図は例を示しています。

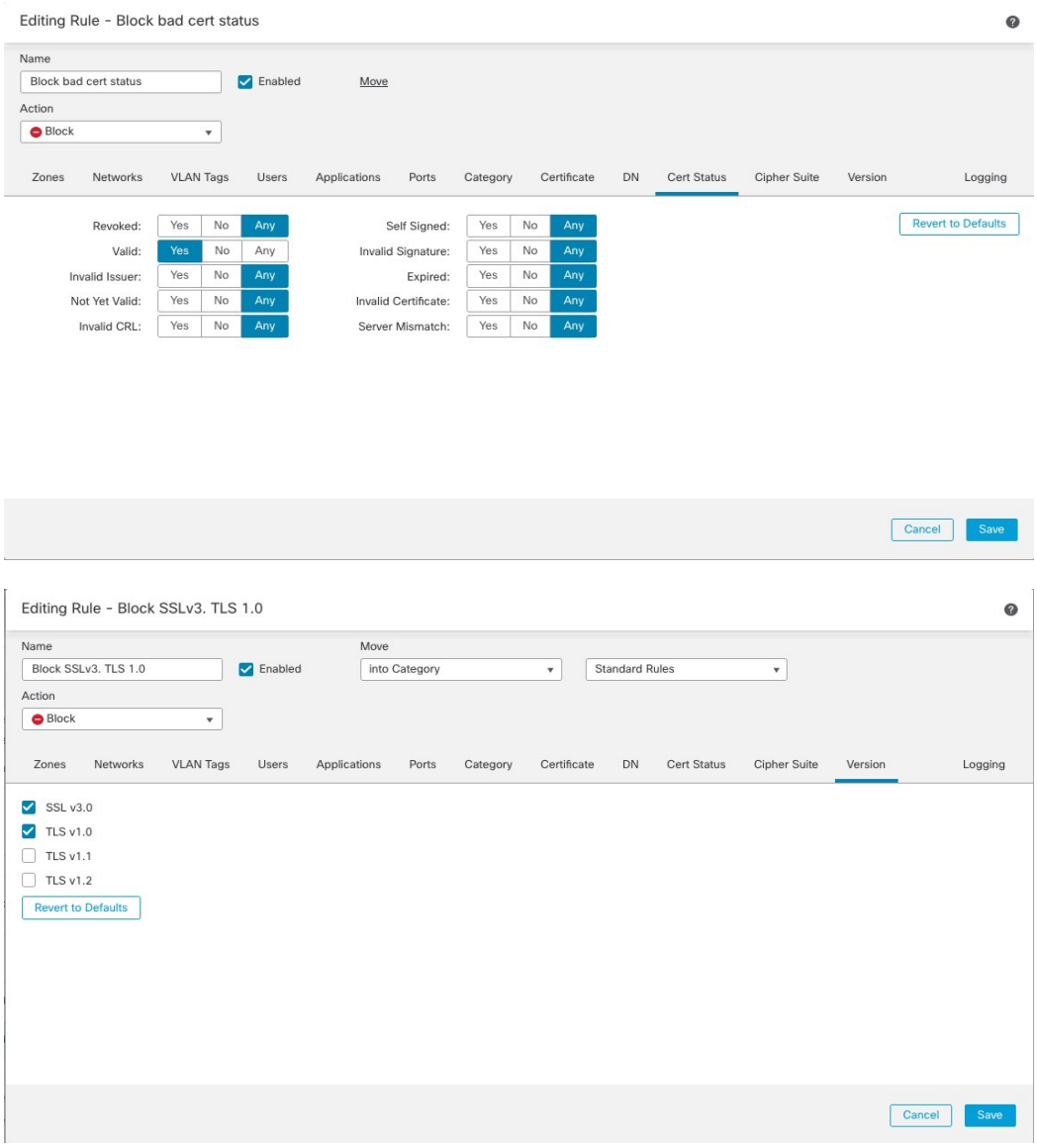


最後の TLS/SSL ルール：証明書とプロトコルバージョンをブロックまたは監視する

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。

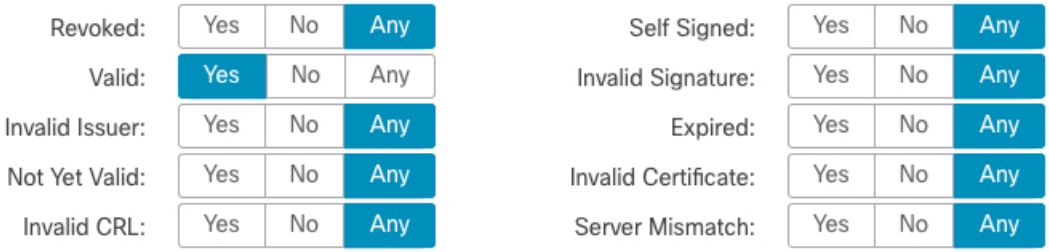
ステップ 11 ポリシーへの変更を保存するには、ページの上部にある [保存（Save）] をクリックします。

例

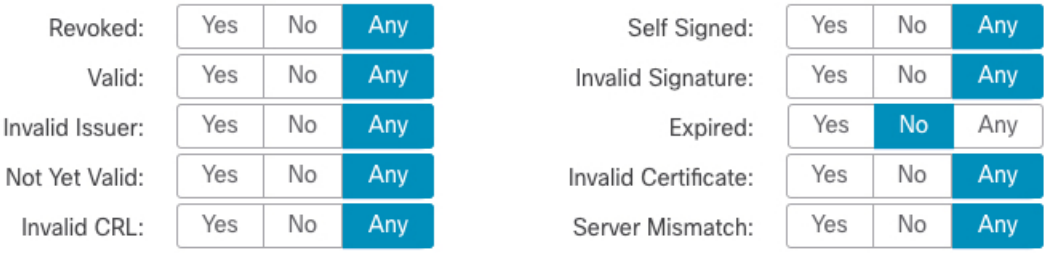
組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書および、Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から提供された CRL をアップロードします。

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

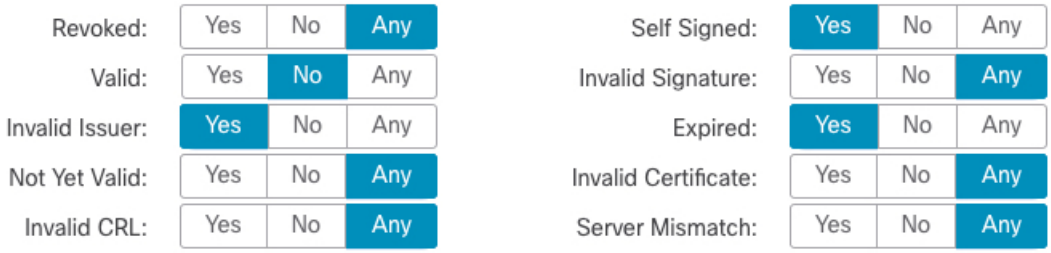
状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。



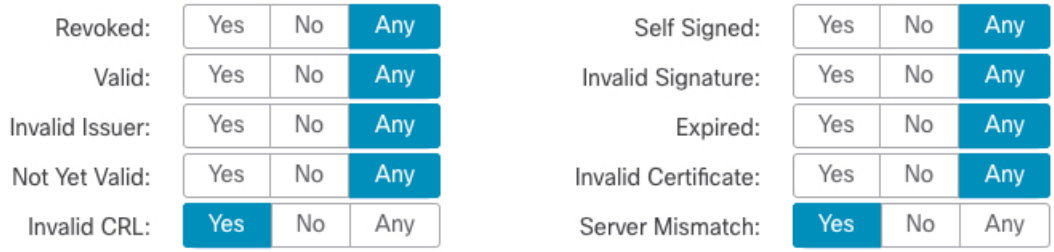
次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合し、そのトラフィックをモニターします。



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。

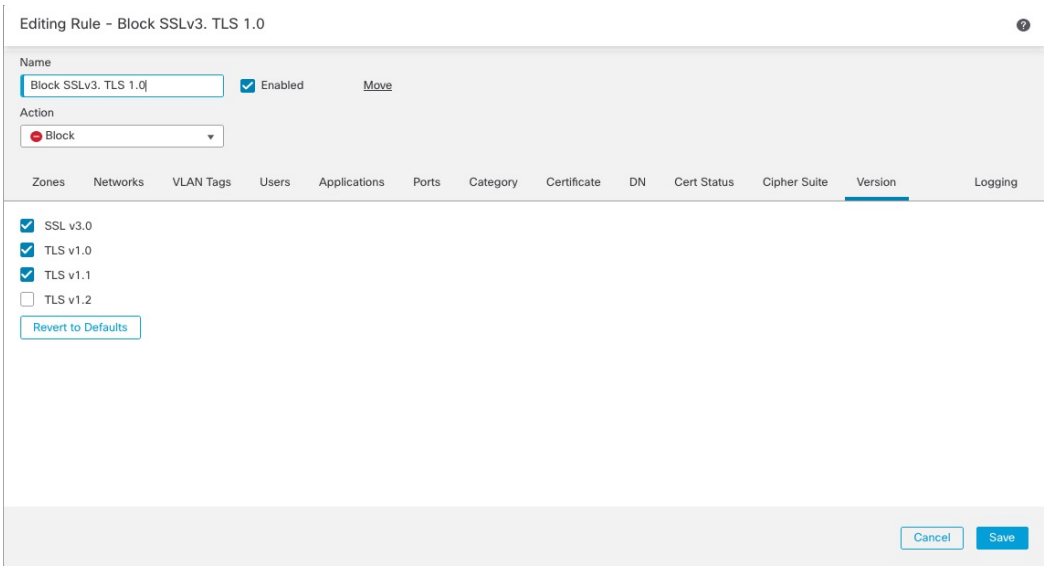
ステップ 6 [ルールの追加（Add Rule）] ダイアログボックスの [名前（Name）] フィールドに、ルールの名前を入力します。

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。

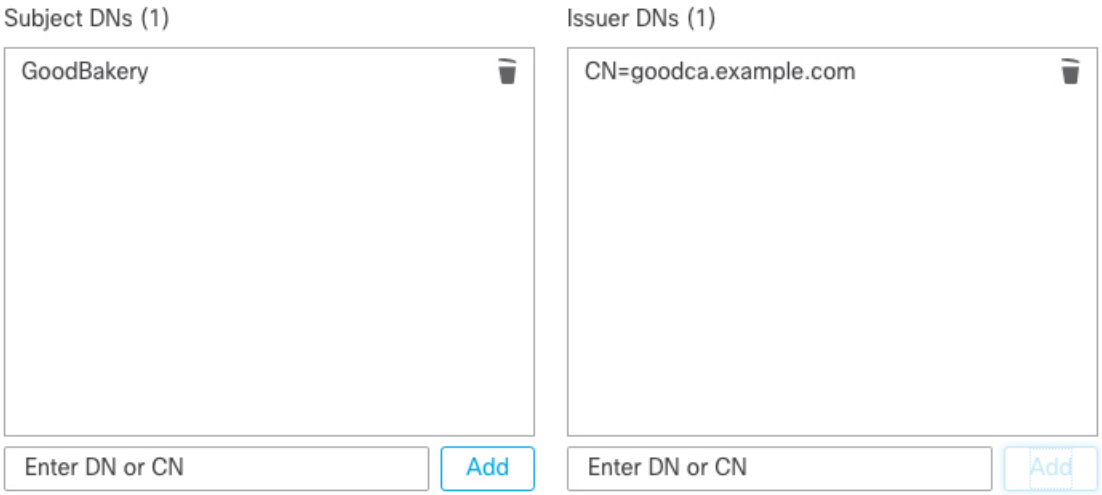
ステップ 13 ルールを追加するか、編集を続けます。

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。