復号ポリシー

ここでは、復号ポリシーの作成、設定、管理、およびロギングの概要を示します。

復号ポリシーについて

A decryption policyにより、ネットワーク上の暗号化トラフィックの処理方法が決まります。1つ以上のdecryption policiesを設定し、a decryption policyをアクセス コントロール ポリシーに関連付けてから、そのアクセス コントロール ポリシーを管理対象デバイスに展開できます。デバイスで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックを処理して検査します。次に TCP 接続上で TLS/SSL 暗号化セッションが識別された場合は、decryption policyが引き継いで暗号化トラフィックの処理および復号が実行されます。

ウィザードを使用した復号ポリシーの作成

ウィザードを使用して、次のタイプの復号ポリシーを作成できます。

- アウトバウンド保護（[復号 - 最署名（Decrypt - Resign）]ルールアクション）。トラフィックがこのルールに一致した場合、システムは CA 証明書を使用してサーバー証明書を再署名してから、中間者（man-in-the-middle）として機能します。

  [復号しない（Do Not Decrypt）] アクションを含む 3 つのルールがポリシーに同時に追加されるため、後で行う手間が省けます。これらのルールは、ポリシーを作成するときに設定する復号の除外項目に対応します（たとえば、証明書のピン留めを使用することが知られているアプリケーションの復号をバイパスするよう選択することができます）。

  詳細については、「アウトバウンド接続保護を使用した復号ポリシーの作成」を参照してください。

- インバウンド保護（[復号 - 既知のキー（Decrypt - Known Key ）] ルールアクション）。1つまたは複数のサーバー証明書と秘密キーペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、システムは適切な秘密キーを使用してセッションの暗号化と復号キーを取得します。

  [復号しない（Do Not Decrypt）] アクションを含む 3 つのルールがポリシーに同時に追加されますが、これらのルールはデフォルトで無効になっています。これらのルールは、ポリシーを作成するときに設定する復号の除外項目に対応します（たとえば、証明書のピン留めを使用することが知られているアプリケーションの復号をバイパスするよう選択することができます）。

  詳細については、「アウトバウンド接続保護を使用した復号ポリシー の作成 （7 ページ）」を参照してください。

- その他の復号ルールアクション（ブロッキングやモニタリングなど）。

  詳細については、「他のルールアクションを使用した復号ポリシーの作成（17ページ）」を参照してください。

ウィザードは、指定した証明書ごとに個別のルールを自動的に作成します。たとえば、インバウンド保護ルールでは、財務部門の内部ネットワークに向かうトラフィックに1つの証明書を指定し、エンジニアリング部門のネットワークに向かうトラフィックには別の証明書を指定することがあります。

ウィザードは、次のように、アウトバウンドおよびインバウンド保護ポリシーの追加ルールを作成します。

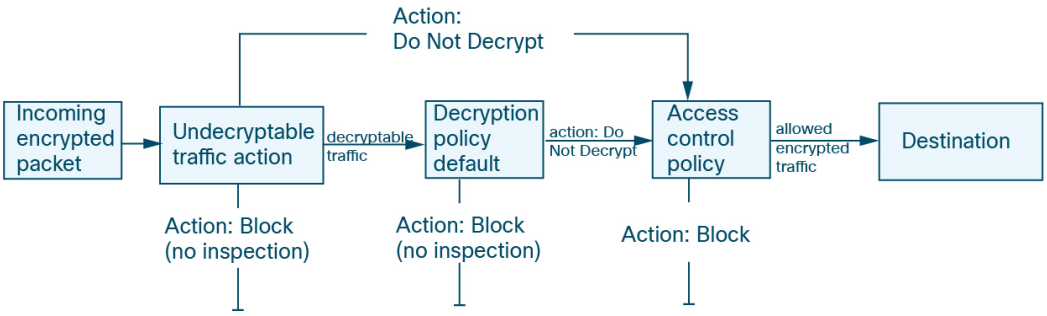
- アウトバウンド保護（[復号 - 再署名（Decrypt - Resign）] ルールアクション）：ウィザードは、ウィザードで指定した例外に一致するトラフィックの [復号しない（Do Not Decrypt）] ルールを作成します。たとえば、復号できないアプリケーション（通常は証明書のピン留めを使用しているアプリケーション）からのトラフィックを復号しないように選択できます。

  トラフィックが最小限の処理でファイアウォールを通過するように [復号しない（Do Not Decrypt）] ルールが復号ポリシーの最初に配置されます。

- インバウンド保護（[復号 - 既知のキー（Decrypt - Known Key ）] ルールアクション）：ウィザードでは例外を選択できませんが、[復号しない（Do Not Decrypt）] ルールがポリシーに追加され、無効になります。これにより、必要に応じて後でこれらの例外を有効にすることができます。

[復号しない（Do Not Decrypt）] ポリシーの例

以下は、[復号しない（Do Not Decrypt）] ルールアクションを使用した復号ポリシーの例です。



最も単純なdecryption policyでは、次の図に示されているように、展開先のデバイスは単一のデフォルトアクションで暗号化トラフィックを処理するように指示されます。デフォルト アクションの設定では、それ以上のインスペクションなしで復号可能トラフィックをブロックするか、復号されていない復号可能トラフィックをアクセス コントロールで検査するように指定できます。システムは、暗号化されたトラフィックを許可するか、またはブロックできます。デバイスは復号できないトラフィックを検出すると、トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないままにして、アクセス コントロールによる検査を行います。

開始するには、の作成復号ポリシー （3 ページ）を参照してください。

Decryption Policies の要件と前提条件

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

の作成復号ポリシー

次のいずれかのタイプの 復号 ポリシーを作成できます。

- アウトバウンド保護ポリシーは、アウトバウンド接続を保護するルールを使用します。つまり、宛先サーバーは保護されたネットワークの外部にあります。このタイプのルールには、[復号 - 再署名（Decrypt - Resign）] ルールアクションがあります。また、指定したトラフィック（証明書のピン留めを使用するトラフィックなど）を除外する **[復号しない（Do Not Decrypt）]** アクションを含む追加のルールも作成します。

  アウトバウンド接続保護を使用した復号ポリシー の作成 （4 ページ）を参照してください

- インバウンド保護ポリシーは、インバウンド接続を保護するルールを使用します。つまり、宛先サーバーは保護されたネットワークの内部にあります。このタイプのルールには、[復号 - 既知のキー（Decrypt - Known Key）] ルールアクションがあります。また、指定したトラフィック（証明書のピン留めを使用するトラフィックなど）を除外する [復号しない（Do Not Decrypt）] アクションを含む追加のルールも作成します。これらのルールは最初は無効になっていますが、必要に応じて後で変更して有効にすることができます。

  アウトバウンド接続保護を使用した復号ポリシー の作成 （7 ページ）を参照してください

- その他のアクション（[復号しない（Do Not Decrypt）]、[ブロック（Block）]、および [リセットしてブロック（Block with Reset）] を含む）。

  「他のルールアクションを使用した 復号ポリシー の作成 （17 ページ）」を参照してください。

アウトバウンド接続保護を使用した復号ポリシー の作成

このタスクでは、アウトバウンド接続を保護するルールを使用して復号ポリシーを作成する方法について説明します。つまり、宛先サーバーは保護されたネットワークの外部にあります。このタイプのルールには、[復号 - 再署名（Decrypt - Resign）] ルールアクションがあります。

復号ポリシーを作成するときは、複数の **[復号 - 既知のキー（Decrypt - Known Key）]** ルールや複数の [復号 - 再署名（Decrypt - Resign）] ルールなど、複数のルールを同時に作成できます。

変更管理を有効にした場合は、復号ポリシーを作成する前にチケットを作成して割り当てる必要があります。復号ポリシーを使用する前に、チケットとすべての関連オブジェクト（認証局など）を承認する必要があります。詳細については、「変更管理チケットの作成」および「変更管理をサポートするポリシーとオブジェクト」を参照してください。

始める前に

アウトバウンド接続を保護する復号ポリシーを作成する前に、管理対象デバイスの内部 CA 証明書をアップロードまたは生成する必要があります。これは、次のいずれかの方法で実行できます。

- **Objects** > **Object Management** > **PKI** > **Internal CAs** に移動して PKI を参照し、内部 CA 証明書オブジェクトを作成します。
- この復号ポリシーの作成時点で実行。

手順

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 **Policies** > **Access Control heading** > **Decryption** をクリックします。

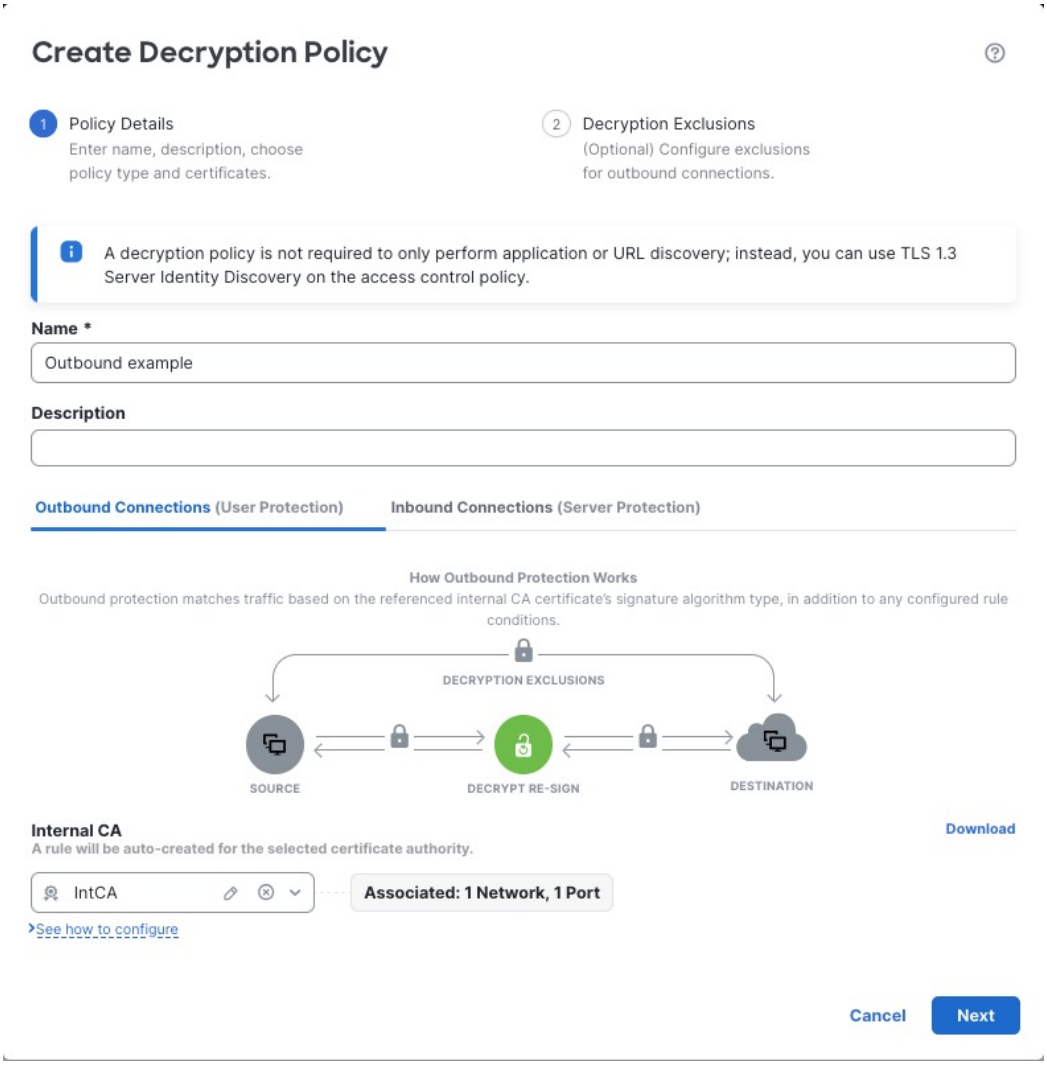
ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

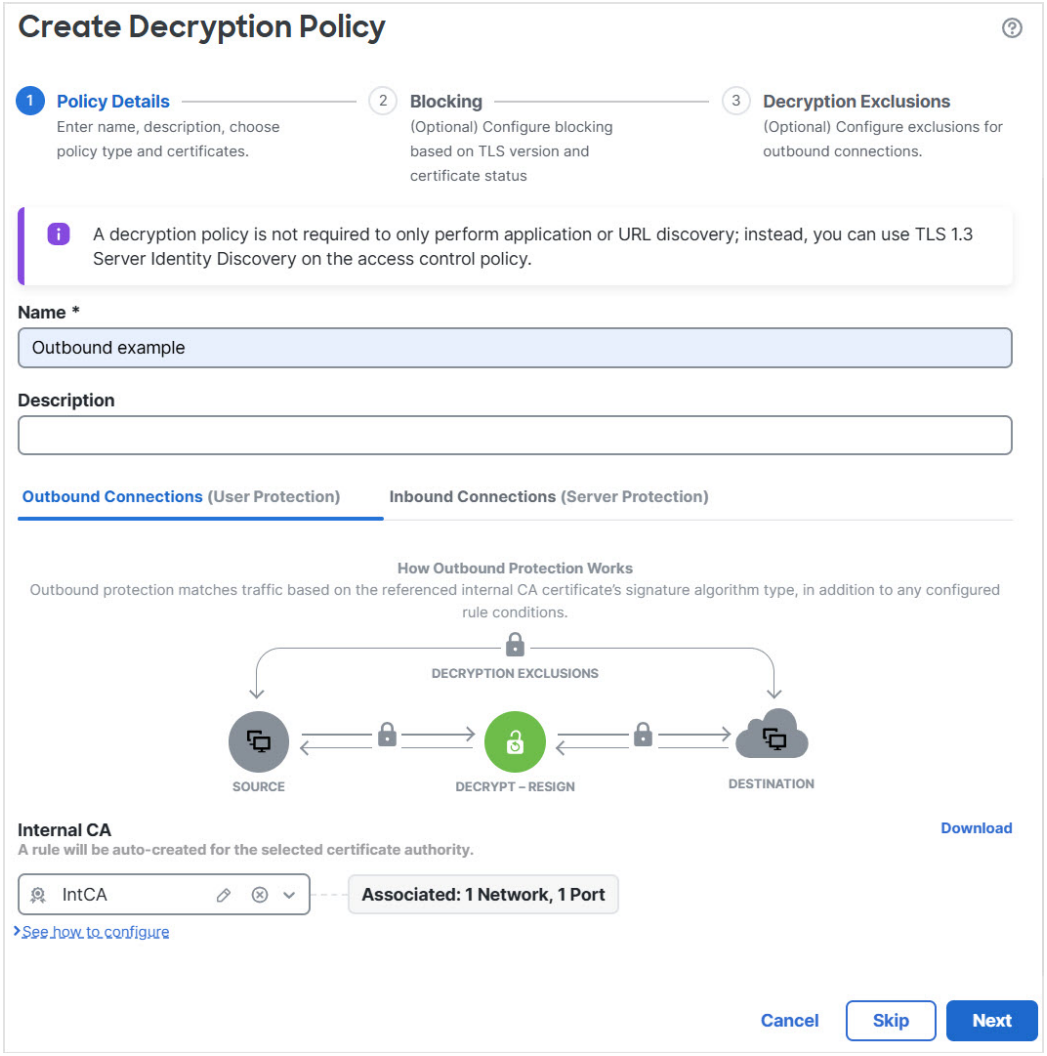
次の文字は、復号ポリシー名には使用できません。

- 先頭のピリオド
- #、;、{、}、=、$、<、>

ステップ 5 [アウトバウンド接続（Outbound Connections）] タブをクリックします。



ステップ 6 [アウトバウンド接続（Outbound Connections）] タブをクリックします。



ステップ 7 [内部CA（Internal CA）] リストから、ルールの証明書をアップロードまたは選択します。

内部証明書の詳細については、「アウトバウンド保護のための内部CAの生成 （15ページ）」と「アウトバウンド保護のための内部 CA のアップロード （16 ページ）」を参照してください。

ステップ 8 （任意）ネットワークとポートを選択します。

詳細については、次を参照してください。

- ネットワークルールの条件
- ポートルールの条件

ステップ 9 [Next] をクリックします。

ステップ 10 接続の 復号ポリシー ブロック （9 ページ）に進みます。

次のタスク

- ルール条件の追加：復号ルール 条件
- デフォルトのポリシーアクションの追加： 復号ポリシー のデフォルトアクション （18 ページ）
- *Cisco Secure Firewall Management Center Administration Guide* の「Logging Connections with a Policy Default Action」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシー 詳細オプション （22 ページ）
- アクセス制御への他のポリシーの関連付けの説明に従って、decryption policyをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開を参照してください。

アウトバウンド接続保護を使用した復号ポリシー の作成

このタスクでは、インバウンド接続を保護するルールを使用して復号ポリシーを作成する方法について説明します。つまり、宛先サーバーは保護されたネットワーク内にあります。このタイプのルールには、[復号 - 既知のキー（Decrypt - Known Key）] ルールアクションがあります。

復号ポリシーを作成するときは、複数の [復号 - 既知のキー（Decrypt - Known Key）] ルールや複数の [復号 - 再署名（Decrypt - Resign）] ルールなど、複数のルールを同時に作成できます。

始める前に

インバウンド接続を保護する復号ポリシーを作成する前に、内部サーバーの内部証明書をオプションとしてアップロードできます。これは、次のいずれかの方法で実行できます。

- **Objects** > **Object Management** > **PKI** > **Internal Certs** に移動し PKI を参照して、内部証明書オブジェクトを作成します。
- この復号ポリシーの作成時点で実行。

変更管理を有効にした場合は、復号ポリシーを作成する前にチケットを作成して割り当てる必要があります。復号ポリシーを使用する前に、チケットとすべての関連オブジェクト（認証局など）を承認する必要があります。詳細については、「変更管理チケットの作成」および「変更管理をサポートするポリシーとオブジェクト」を参照してください。

手順

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 **Policies** > **Access Control heading** > **Decryption** をクリックします。

ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

次の文字は、復号ポリシー名には使用できません。

- 先頭のピリオド
- #、;、{、}、=、$、<、>

ステップ 5 [内部証明書（Internal Certificates）] リストから、ルールの証明書をアップロードまたは選択します。

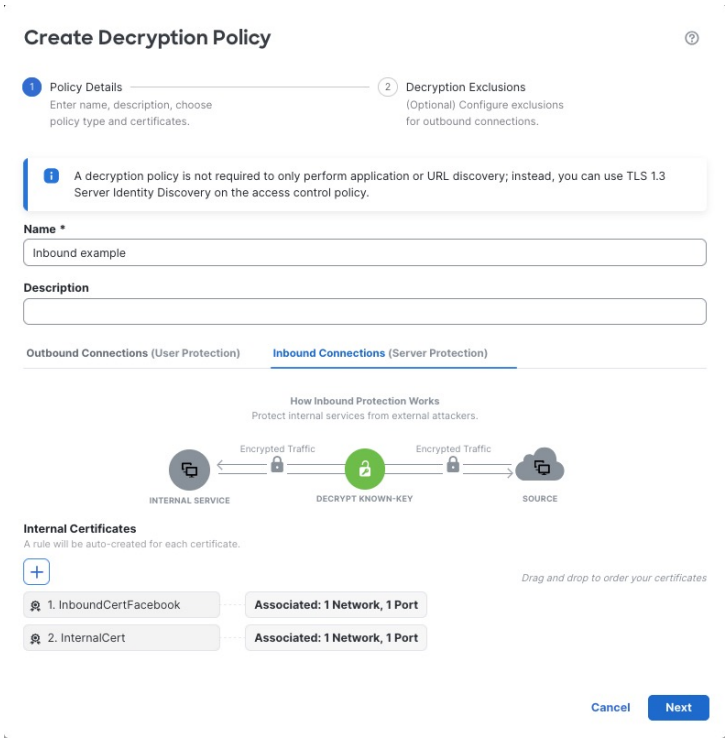
内部 CA 証明書の詳細については、「内部認証局オブジェクト」を参照してください。

ステップ 6 （任意）ネットワークとポートを選択します。

詳細については、次を参照してください。

- ネットワークルールの条件
- ポートルールの条件

ステップ 7 [インバウンド接続（Inbound Connections）] タブをクリックします。



ステップ 8 [Next] をクリックします。

ステップ 9 接続の 復号ポリシー ブロック （9 ページ） に進みます。

ステップ 10 復号ポリシー の除外 （10 ページ）に進みます。

次のタスク

- ルール条件の追加：復号ルール 条件
- デフォルトのポリシーアクションの追加： 復号ポリシー のデフォルトアクション （18 ページ）
- *Cisco Secure Firewall Management Center Administration Guide* の「*Logging Connections with a Policy Default Action*」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシー 詳細オプション （22 ページ）
- アクセス制御への他のポリシーの関連付けの説明に従って、decryption policyをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開を参照してください。

接続の 復号ポリシー ブロック

ここでは、復号ポリシー の作成中に、TLS バージョンとサーバー証明書ステータスがセキュアでないサーバーへの接続をブロックする方法について詳しく説明します。復号ポリシーには [リセットしてブロック（Block with Reset）] ルールが含まれていますが、デフォルトで無効になっています。

手順

ステップ 1 以下に記載されているタスクを実行します。

- アウトバウンド接続保護を使用した復号ポリシー の作成 （4 ページ）
- アウトバウンド接続保護を使用した復号ポリシー の作成 （7 ページ）

ステップ 2 [ブロッキング（Blocking）] ページには、次のオプションがあります。デフォルトでは、復号ポリシーアクションのすべてのオプションが無効 になっています。

- [TLSバージョンに基づいて接続をブロックする（Block connections based on TLS version）]：セキュアでない TLS バージョンを使用するサーバーへの接続をブロックするには、このチェックボックスをオンにします。デフォルトでは、脆弱であることが知られている **SSL v3.0**、**TLS v1.0**、および **TLS v1.1** が選択されます。ドロップダウンリストから他のバージョンを選択できます。
- [サーバー証明書のステータスに基づいて接続をブロックする（Block connections based on server certificate status）]：サーバー証明書のステータスがセキュアでないサーバーへの接続をブロックするには、このチェックボックスをオンにします。デフォルトでは、[署名が無効（Invalid Signature）]、[期限切れ（Expired）]、[まだ無効（Not Yet Valid）]、および [無効な証明書（Invalid Certificate）] が選択されています。ドロップダウンリストから他のステータスを選択できます。

Delete (✕) をクリックして選択を削除するか、[デフォルトにリセット（Reset to default）] をクリックしてデフォルトの選択に戻します。

ステップ 3 [Next] をクリックします。

次のタスク

復号ポリシー の除外 （10 ページ）に進みます。

復号ポリシー の除外

このタスクでは、特定のタイプのトラフィックを復号から除外する方法について説明します。該当するトラフィックについて、復号ポリシーで [復号しない（Do not decrypt）] ルールを作成します。このルールは、当初アウトバウンド復号ポリシー（つまり、[復号 - 再署名（Decrypt - Resign）] ポリシーアクションを使用するポリシー）に対してのみ有効になっています。

始める前に

アウトバウンド接続を保護する 復号ポリシー を作成する前に、管理対象デバイスの内部 CA 証明書をアップロードする必要があります。これは、次のいずれかの方法で実行できます。

- **Objects** > **Object Management** > **PKI** > **Internal CAs** に移動して PKI を参照し、内部 CA 証明書オブジェクトを作成します。
- この復号ポリシーの作成時点で実行。

手順

ステップ 1 次で説明されているタスクを完了します。

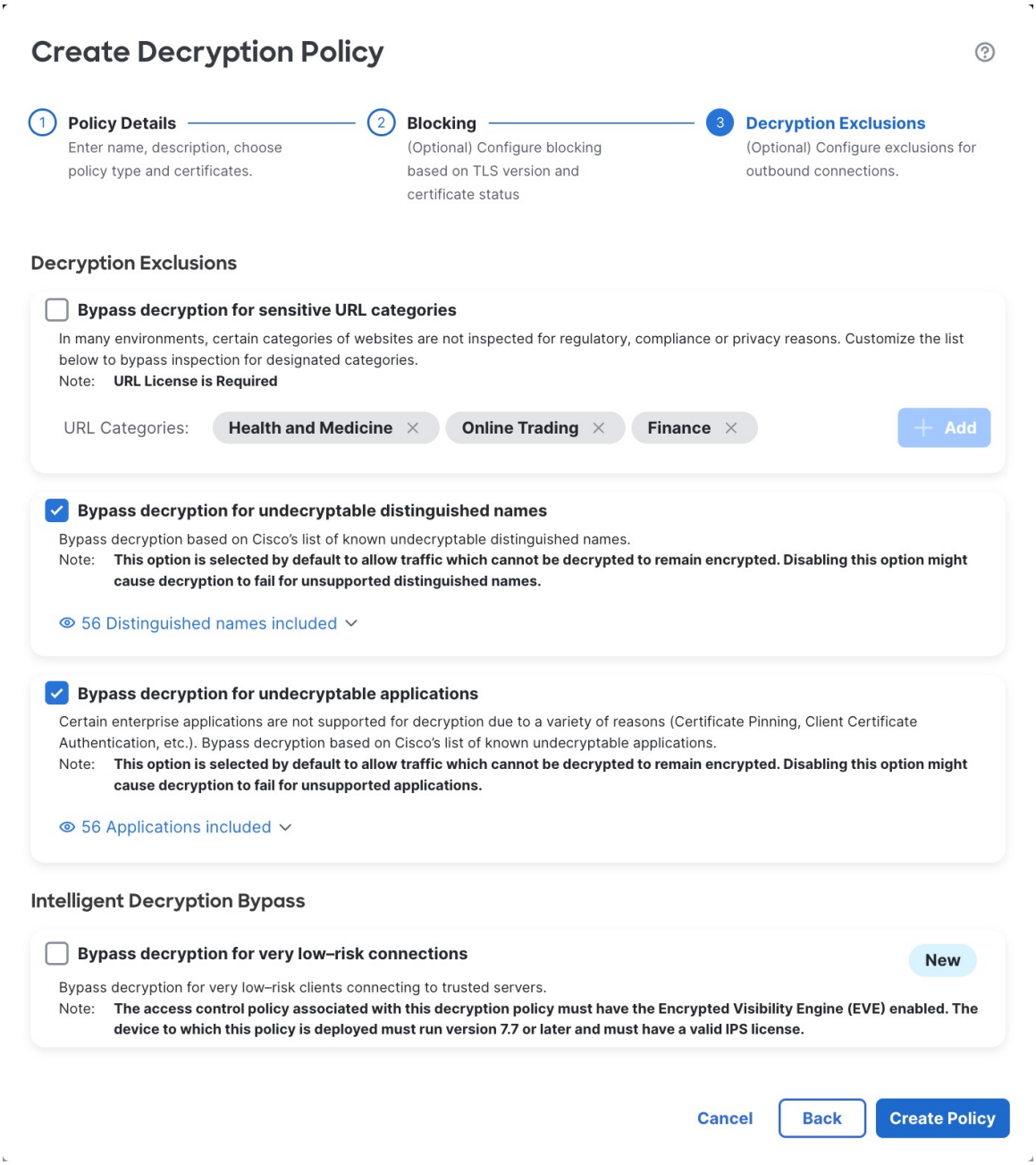
- アウトバウンド接続保護を使用した復号ポリシー の作成 （4 ページ）
- 詳細については、アウトバウンド接続保護を使用した復号ポリシー の作成 （7 ページ）を参照してください。

ステップ 2 除外ページには次のオプションがあります。すべてのオプションは、アウトバウンド保護ポリシー（[復号 - 再署名（Decrypt - Resign）] ルールアクション）に対して 有効 になり、他のすべての復号ポリシーアクションに対しては 無効 になります。

項目	説明
機密URLカテゴリの復号のバイパス（Bypass decryption for sensitive URL categories）	指定されたカテゴリからのトラフィックを復号しない場合は、このチェックボックスをオンにします。お住まいの地域の法律によっては、特定のトラフィック（金融や健康関連など）の復号が禁止されている場合があります。詳細については、お住まいの地域の当局にお問い合わせください。 カテゴリを追加するには、[追加（Add）]をクリックします。 カテゴリを削除するには、 **Delete** ( ) をクリックします。
復号不能な識別名の復号のバイパス（Bypass decryption for undecryptable distinguished names）	証明書の再署名によって接続が失敗する可能性があるためトラフィックを復号しない場合は、このボックスをオンにします。通常、この動作は 証明書のピン留めに関連付けられています。この操作については で説明されています。TLS/SSL 証明書のピン留めのガイドライン 復号できない識別名のリストは、シスコが管理しています。
復号不能なアプリケーションの復号のバイパス（Bypass decryption for undecryptable applications）	証明書の再署名によって接続が失敗する可能性があるためトラフィックを復号しない場合は、このボックスをオンにします。 通常、この動作は 証明書のピン留めに関連付けられています。この操作については で説明されています。TLS/SSL 証明書のピン留めのガイドライン 復号できないアプリケーションは、脆弱性データベース（VDB）で自動的に更新されます。すべてのアプリケーションのリストは、Cisco Secure Firewall アプリケーションディテクタのページで確認できます。シスコが復号できないと判断したアプリケーションは、**undecryptable** タグで識別されています。 復号できないアプリケーションのリストは、シスコによって管理されています。

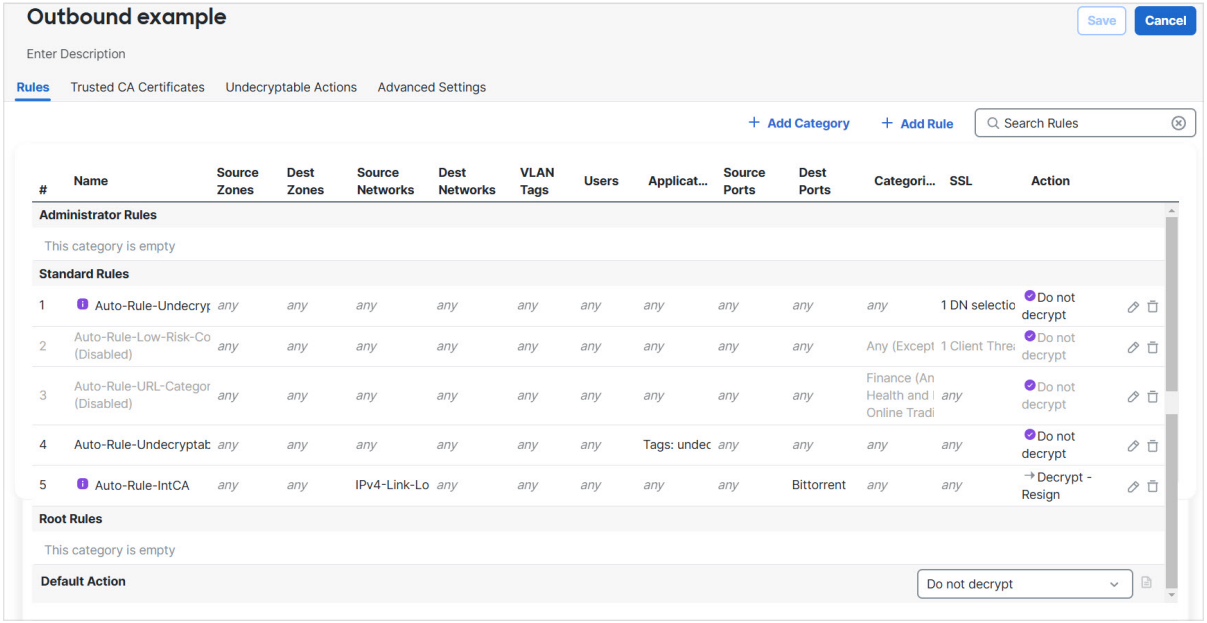
項目	説明
[特に低リスクの接続では復号をバイパス（Bypass decryption for very low-risk connections）]	Encrypted Visibility Engine（EVE）およびURL カテゴリレピュテーションによって決定されたクライアントの脅威信頼レベルに基づいて、信頼できるサーバーに接続している非常に低リスクのクライアントのトラフィックを復号しない場合は、このチェックボックスをオンにします。 [Auto-Rule-Low-Risk-Connections]：[復号しない（Do Not Decrypt）] ルールが作成され、新しい復号ポリシーで有効になっています。 [特に低リスクの接続では複合をバイパス（Bypass decryption for very low-risk connections）] オプションを使用するには、対応するアクセス コントロール ポリシーで EVE を有効にする必要があります。また、管理対象デバイスは、有効な IPS ライセンスでバージョン 7.7 以降を実行している必要があります。 アプリケーション リスクと関連性の分類の現在のリストを確認するには、[セキュア ファイアウォール アプリケーション ディテクタ（Secure Firewall Application Detectors）]に移動します。

次の図は、デフォルトのオプションを示しています。



ステップ 3 [ポリシーの作成（Create Policy）] をクリックします。

次の図は、アウトバウンド保護ポリシーの例を示しています。



前の例では、ルールの除外の選択に対応する [復号しない（Do Not Decrypt）] ルールが、[復号 - 再署名（Decrypt - Resign）] ルールの前に自動的に追加されます。機密 URL カテゴリのルールは、デフォルトでは除外が無効になっているため、無効になっています。[機密URLカテゴリの復号のバイパス（Bypass decryption for sensitive URL categories）] チェックボックスをオンにした場合、このルールは有効になっています。

ステップ 4 [ポリシーの作成（Create Policy）] をクリックします。

次のタスク

- ルール条件の追加：復号ルール 条件
- デフォルトのポリシーアクションの追加： 復号ポリシー のデフォルトアクション （18 ページ）
- *Cisco Secure Firewall Management Center Administration Guide* の「Logging Connections with a Policy Default Action」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシー 詳細オプション （22 ページ）
- アクセス制御への他のポリシーの関連付けの説明に従って、decryption policyをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開を参照してください。

アウトバウンド保護のための内部 CA の生成

このタスクでは、アウトバウンド接続を保護する復号ルールを作成するときに、オプションで内部認証局を生成する方法について説明します。CSR への応答として発行された署名付き証明書のアップロードの説明に従って、**Objects** > **Object Management** を使用してこれらのタスクを実行することもできます。

始める前に

内部認証局オブジェクトに記載されている内部認証局オブジェクトを生成するための要件をよく理解してください。

手順

ステップ 1 [内部CA（Internal CA）] リストから、**[新規作成（Create New）]** > **[CAの生成（Generate CA）]** をクリックします。

ステップ 2 内部 CA に [名前（Name）] を付け、2 文字の [国名（Country Name）]を指定します。

ステップ 3 [自己署名（Self-Signed）]または [CSR] をクリックします。

これらのオプションの詳細については、内部認証局オブジェクト を参照してください。

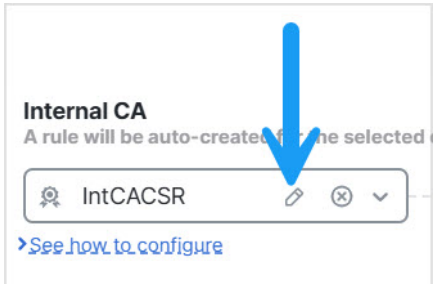
ステップ 4 表示されたフィールドに必要な情報を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [CSR] を選択した場合は、署名要求が完了したら、次のように [証明書のインストール（Install Certificate）] をクリックします。

a) この手順の前のステップを繰り返します。

b) [内部CA（Internal CA）] リストの CA を次のように編集します。



c) [Install Certificate] をクリックします。

d) 画面に表示される指示に従ってタスクを完了します。

ステップ 7 「アウトバウンド接続保護を使用した復号ポリシー の作成 （4 ページ）」の説明に従って、ポリシーの作成を続行します。

アウトバウンド保護のための内部 CA のアップロード

このタスクでは、アウトバウンド接続を保護する復号ルールを作成するときに、オプションで内部認証局をアップロードする方法について説明します。CSR への応答として発行された署名付き証明書のアップロードの説明に従って、**Objects** > **Object Management** を使用してこれらのタスクを実行することもできます。

始める前に

内部認証局オブジェクトに記載されている内部認証局オブジェクトを生成するための要件をよく理解してください。

手順

ステップ 1 [内部CA（Internal CA）] リストから、**[新規作成（Create New）]** > **[CAのアップロード（Upload CA）]**をクリックします。

ステップ 2 内部 CA に名前を付けます。

ステップ 3 表示されたフィールドに、証明書とその秘密鍵を貼り付けるか、参照して見つけます。

ステップ 4 CA にパスワードが設定されている場合は、[暗号化（Encrypted）] チェックボックスをオンにして、隣のフィールドにパスワードを入力します。

ステップ 5 「アウトバウンド接続保護を使用した復号ポリシー の作成 （4 ページ）」の説明に従って、ポリシーの作成を続行します。

アウトバウンド保護のための内部証明書のアップロード

このタスクでは、インバウンド接続を保護する復号ルールを作成するときに、内部認証をアップロードする方法について説明します。CA 証明書および秘密キーのインポートで説明されているように、**Objects** > **Object Management** を使用して内部証明書をアップロードすることもできます。

始める前に

内部認証局オブジェクト で説明されているいずれかの形式の内部認証があることを確認してください。

手順

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 **Policies** > **Access Control heading** > **Decryption** をクリックします。

ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 [名前（Name）] フィールドにポリシーの名前を入力し、[説明（Description）] フィールドに任意の説明を入力します。

ステップ 5 [インバウンド接続（Inbound Connections）] タブをクリックします。

ステップ 6 [内部証明書（Internal Certificates）] リストから、**Add** (+) をクリックします。

ステップ 7 内部証明書オブジェクトが存在する場合は、その名前をクリックします。

ステップ 8 それ以外の場合は、**[アップロード（Upload）]**をクリックします。

ステップ 9 必要な情報を入力します。

内部証明書オブジェクトの追加を参照してください。

ステップ 10 「アウトバウンド接続保護を使用した復号ポリシー の作成 （7 ページ）」の説明に従って、復号ポリシーの作成を続行します。

他のルールアクションを使用した 復号ポリシー の作成

[復号しない（Do Not Decrypt）]、**[ブロック（Block）]**、**[リセットしてブロック（Block With Reset）]**、または **[モニター（Monitor）]** ルールアクションを使用して復号ルールを作成するには、復号ポリシーを作成、編集して、ルールに追加します。

復号ポリシー を作成するときは、複数の **[復号 - 既知のキー（Decrypt - Known Key）]**、複数の **[復号 - 再署名（Decrypt - Resign）]** ルールなど、複数のルールを同時に作成できます。

変更管理を有効にした場合は、復号ポリシーを作成する前にチケットを作成して割り当てる必要があります。復号ポリシーを使用する前に、チケットとすべての関連オブジェクト（認証局など）を承認する必要があります。詳細については、「変更管理チケットの作成」および「変更管理をサポートするポリシーとオブジェクト」を参照してください。

手順

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 **Policies** > **Access Control heading** > **Decryption** をクリックします。

ステップ 3 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

次の文字は、復号ポリシー名には使用できません。

- 先頭のピリオド
- #、;、{、}、=、$、<、>

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 バイパスページは情報提供のみを目的としています。他のタイプの復号（[ブロック（Block）] など）のトラフィックをバイパスすることはできません。

ステップ 6 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 7 ポリシーが作成されるまで待機します。

ステップ 8 復号ポリシー名の横にある **Edit** ( )をクリックします。

ステップ 9 [ルールの追加（Add Rule）] をクリックします。

ステップ 10 ルールに [名前（Name）] を付けます。

ステップ 11 詳細については、[アクション（Action）] リストからルールアクションをクリックし、次のいずれかのセクションを参照してください。

- Decryption rule 復号アクションを実行しない
- Decryption ruleのブロック アクション
- Decryption ruleのモニター アクション

ステップ 12 [保存（Save）] をクリックします。

次のタスク

- ルール条件の追加：復号ルール 条件
- デフォルトのポリシーアクションの追加： 復号ポリシー のデフォルトアクション （18 ページ）
- *Cisco Secure Firewall Management Center Administration Guide* の「Logging Connections with a Policy Default Action」の説明に従って、デフォルトアクションのロギングオプションを設定します。
- 詳細ポリシーのプロパティの設定：復号ポリシー 詳細オプション （22 ページ）
- アクセス制御への他のポリシーの関連付けの説明に従って、decryption policyをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します設定変更の展開を参照してください。

復号ポリシー のデフォルトアクション

復号ポリシーのデフォルトアクションは、ポリシーのモニター以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。decryption rules がまったく含まれない 復号ポリシー を展開する場合、ネットワーク上のすべての復号可能トラフィックの処理方法が、デフォルトアクションで決定されます。デフォルトアクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

ポリシーのデフォルト アクションを設定する方法：

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。

2. **Policies** > **Access Control heading** > **Decryption** をクリックします。
3. decryption policyの名前の横にある **Edit** (✎) をクリックします。
4. [デフォルトアクション（Default Action）] 行で、リストから次のいずれかのアクションをクリックします。

表 *1 : Decryption policy* のデフォルトアクション

デフォルト アクション	暗号化トラフィックに対して行う処理
ブロック（Block）	それ以上のインスペクションは行わずに TLS/SSL セッションをブロックします。
Block with reset	それ以上のインスペクションは行わずに TLS/SSL セッションをブロックし、TCP 接続をリセットします。トラフィックに UDP のようなコネクションレス型プロトコルが使用される場合は、このオプションを選択します。この場合、コネクションレス型プロトコルにより、リセットされるまで接続の再確立が試みられます。 また、このアクションでは、ブラウザの接続リセット エラーも表示されるため、接続がブロックされたことがユーザーに通知されます。
復号しない（Do not decrypt）	アクセス コントロールを使用して暗号化トラフィックを検査します。

復号できないトラフィックのデフォルト処理オプション

表 *2 :* 復号化できないトラフィック タイプ

タイプ	説明	デフォルト アクション	使用可能なアクション
圧縮されたセッション（Compressed Session）	TLS/SSL セッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）

タイプ	説明	デフォルト アクション	使用可能なアクション
SSLv2 セッション	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、ClientHello メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 であることに注意してください。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Unknown Cipher Suite	システムが認識できない暗号スイートです。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Unsupported Cipher Suite	検出された暗号スイートに基づく復号化を、システムはサポートしていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
セッションが未キャッシュ（Session not cached）	TLS/SSL セッションでセッションの再利用が有効化されており、クライアントとサーバがセッション識別子を使ってセッションを再確立しているのに、システムでセッション識別子がキャッシュされていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
ハンドシェイク エラー（Handshake Errors）	TLS/SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Decryption Errors	トラフィックの復号化中にエラーが発生しました。	ブロック（Block）	ブロック（Block） Block with Reset

a decryption policyを最初に作成する場合、デフォルトアクションによって処理される接続のログは、デフォルトでは無効化されています。復号化できないトラフィックの処理ではデフォルトアクションのログ設定も適用されるため、復号化できないトラフィック用のアクションで処理される接続のログは、デフォルトでは無効化されています。

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できないことに注意してください。詳細については、復号ルール 注意事項と制約事項を参照してください。

復号ポリシーが TCP ステートバイパスを使用するアクセス コントロール ポリシーに関連付けられている場合、一致するトラフィックは、ポリシーで設定されている [ハンドシェイクエラー（Handshake Errors）] に対する [復号不可のアクション（Undecryptable Actions）] に基づいて処理されます。

たとえば、復号ポリシーの [ハンドシェイクエラー（Handshake Errors）] が [ブロック（Block）] に設定されている場合、ルールに一致するトラフィックはブロックされ、接続イベントのアクションはハンドシェイクエラーとして報告されます。

TCP ステートバイパスの詳細については、次を参照してください。

- TCP ステート バイパスの設定
- Bypass TCP state checks for asymetrical routing (TCP state bypass)

関連トピック

復号できないトラフィックのデフォルト処理を設定する （21 ページ）

復号できないトラフィックのデフォルト処理を設定する

システムによる復号や検査ができない特定タイプの暗号化トラフィックを処理するために、復号できないトラフィックのアクションを復号ポリシーレベルで設定できます。decryption rules を含まない復号ポリシーを展開する場合、ネットワーク上のすべての復号できない暗号化トラフィックの処理方法は、復号できないトラフィックのアクションによって決まります。

復号できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロック。
- 接続をブロックした後でリセットする。接続がブロックされるまで接続を試行し続ける UDP などのコネクションレス型プロトコルの場合、このオプションをお勧めします。
- アクセス コントロールを使用して暗号化トラフィックを検査します。
- 復号ポリシーからデフォルトのアクションを継承します。

手順

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 **Policies** > **Access Control heading** > **Decryption** をクリックします。

ステップ 3 decryption policyの名前の横にある **Edit** (✎) をクリックします。

ステップ 4 decryption policyエディタで、[復号できないアクション（Undecryptable Actions）] をクリックします。

ステップ 5 各フィールドで、decryption policyのデフォルトアクションを選択するか、復号できないタイプのトラフィックに対して実行する別のアクションを選択します。詳細については、復号できないトラフィックのデフォルト処理オプション （19 ページ）と 復号ポリシー のデフォルトアクション （18 ページ）を参照してください。

ステップ 6 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 復号できないトラフィックのアクションで処理される接続に関するデフォルトロギングを設定します。*Cisco Secure Firewall Management Center Administration Guide*の「*Logging Connections with a Policy Default Action*」を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。

復号ポリシー 詳細オプション

復号ポリシー の **[詳細設定（Advanced Settings）]** ページには、ポリシーが適用される Snort 3 用に設定されたすべての管理対象デバイスに適用されるグローバル設定があります。

復号ポリシー 詳細設定は、以下を実行する管理対象デバイスではすべて無視されます。

- 7.1 より前のバージョン
- Snort 2

[ESNIを要求するフローをブロックする（Block flows requesting ESNI）]

Encrypted Server Name Indication（ESNI（提案の草案へのリンク））は、クライアントが要求している内容を TLS 1.3 サーバーに伝える方法です。https://tools.ietf.org/html/draft-ietf-tls-esniSNI は暗号化されており、システムではサーバーを判別できないため、SNI 接続は必要に応じてブロックできます。

HTTP/3 アドバタイズメントを無効にする

このオプションを選択すると、TCP 接続の ClientHello から HTTP/3（RFC 9114）が削除されます。HTTP/3 は QUIC トランスポートプロトコルの一部であり、TCP トランスポートプロトコルではありません。クライアントによる HTTP/3 のアドバタイジングをブロックすると、QUIC 接続に埋め込まれている可能性のある攻撃や回避の試行に対する保護が提供されます。

信頼できないサーバー証明書をクライアントに伝播する

これは、[復号-再署名（Decrypt - Resign）] ルールアクションに一致するトラフィックにのみ適用されます。

このオプションを有効にすると、サーバー証明書が信頼されていない場合に、管理対象デバイスの認証局（CA）がサーバーの証明書の代わりに使用されます。信頼されていないサーバー証明書とは、Secure Firewall Management Center で信頼できる CA としてリストされていない証明書です。（**Objects** > **Object Management** > **PKI** > **Trusted CAs**）。

TLS 1.3復号の有効化

TLS 1.3 接続に復号ルールを適用するかどうか。このオプションを有効にしない場合、復号ルールは TLS 1.2 以下のトラフィックにのみ適用されます。「TLS 1.3 復号のベストプラクティス（25 ページ）」を参照してください。

[適応型TLSサーバーアイデンティティプローブの有効化（Enable adaptive TLS server identity probe）]

TLS 1.3 復号が有効な場合、自動的に有効になります。 プローブは、サーバーとの部分的な TLS 接続であり、その目的はサーバー証明書を取得してキャッシュすることです。（証明書がすでにキャッシュされている場合、プローブは確立されません。）

復号ポリシーが関連付けられているアクセス コントロール ポリシーで TLS 1.3 サーバーアイデンティティ検出が無効になっている場合、サーバー名指定（SNI）の使用が試行されますが、これは信頼性が高くありません。

適応型 TLS サーバー アイデンティティ プローブは、以前のリリースのようにすべての接続では発生せず、次のいずれかの条件で発生します。

- 証明書の発行者：復号ルールの DN ルール条件で発行者 DN の値が一致する場合に一致します。

  詳細については、識別名（DN）ルールの条件を参照してください。

- 証明書ステータス：復号ルールでいずれかの証明書ステータス条件が一致する場合に一致します。

  詳細については、証明書ステータスの Decryption rule条件を参照してください。

- 内部/外部証明書：内部証明書は、[復号-既知のキー（Decrypt - Known Key）] ルールアクションで使用される証明書と照合できます。外部証明書は、証明書ルール条件で照合できます。

  詳細については、既知のキーでの復号（着信トラフィック）および証明書ルールの条件を参照してください。

- アプリケーション ID：アクセス コントロール ポリシーまたは復号ポリシーのアプリケーションルール条件と照合できます。

  詳細については、アプリケーションルールの条件を参照してください。

- URL カテゴリ：アクセス コントロール ポリシーの URL ルール条件と照合できます。

詳細については、URL ルール条件を参照してください。

（注） [適応型TLSサーバーでの検出モードの有効化（Enable adaptive TLS server discovery mode）] は、AWS に展開されたどの Secure Firewall Threat Defense Virtual でもサポートされていません。Secure Firewall Management Center で管理されているそのような管理対象デバイスがある場合、接続イベント **PROBE_FLOW_DROP_BYPASS_PROXY** は、デバイスがサーバー証明書の抽出を試みるたびに増加します。

QUIC復号の有効化

QUIC プロトコルを介した HTTP/3 を使用する接続に復号ルールを適用するかどうか。QUIC 接続を復号すると、システムは侵入、マルウェア、またはその他の問題についてセッションの内容を検査できます。また、アクセス コントロール ポリシーの特定の基準に基づいて、復号された QUIC 接続のきめ細かい制御とフィルタリングを適用することもできます。QUIC のサポートは、RFC 9000、9001、9002、9114、9204 に準拠しています。

QUIC 復号を実装する場合は、次の点を考慮してください。

- 高可用性またはクラスタ化されたデバイスでは、QUIC 復号は、接続が同じノード上にとどまっている場合にのみ機能します。接続がフェールオーバーした場合、または別のノードに転送された場合、接続は切断され、再度確立する必要があります。マルチインスタンスは制限なしでサポートされています。
- QUIC トラフィックに適用されるルールには、宛先ポート 443 の UDP プロトコルが含まれます。
- QUIC トラフィックに適用されるアクセス制御ルールには、HTTP/3 または QUIC プロトコルが明示的または暗黙的に含まれます。

QUIC 復号には次の制限が適用されます。

- QUIC 復号は、Firewall Threat Defense 7.6 以降にのみ適用されます。下位リリースを実行しているデバイスは、QUIC 接続を復号できません。
- Chromium スタック（Google Chrome、Opera、Edge）を使用するブラウザからの接続は、アウトバウンドトラフィックに対して復号できません。ただし、同じブラウザからの着信トラフィックは復号できます。
- RFC 9000 に記載されている接続の移行はサポートされません。QUIC の接続 ID の概念により、エンドポイントはアドレスが変更された場合に同じ接続を保持できます。
- キーの更新、セッションの再開、および QUIC バージョン 2 はサポートされません。
- インタラクティブブロックおよびリセット付きインタラクティブブロック（アクセス コントロール ルール内）はサポートされていません。これらのアクションは、[ブロック（Block）] および [リセット付きブロック（Block with Reset）] として機能します。

- 接続ごとのアクティブな接続 ID は 5 に制限されます。必要に応じて、デバイスの CLI で **system support quic-tuning** および **system support quic-tuning-reset** コマンドを使用して、これらの制限を変更できます。

TLS 1.3 復号のベストプラクティス

推奨事項：詳細オプションを有効にする場合

復号ポリシーとアクセス コントロール ポリシーの両方に、トラフィックが復号されているかどうかに関係なく、トラフィックの処理方法に影響する詳細オプションがあります。

詳細オプションは次のとおりです。

- 復号ポリシー：
  - TLS 1.3 復号
  - TLS 適応型サーバーのアイデンティティプローブ
- アクセス コントロール ポリシー：TLS 1.3 サーバーアイデンティティ検出

  アクセス コントロール ポリシー設定は、復号ポリシー設定よりも優先されます。

次の表を使用して、有効にするオプションを決定します。

TLS 適応型サーバーのアイデンティティプローブ設定（復号ポリシー）	TLS 1.3 サーバーアイデンティティ検出設定（アクセス コントロール ポリシー）	結果	推奨される状況
有効	無効	復号ポリシーに復号ポリシー詳細オプション（22ページ）で指定されたいずれかのルール条件が含まれ、かつサーバー証明書がキャッシュされていない場合に適応プローブが送信されます。	• アクセスコントロールルールでアプリケーション条件または URL 条件を使用していない • トラフィックを復号している
有効	有効	サーバー証明書がキャッシュされていない場合、プローブは常に送信されます。	アクセスコントロールルールに URL 条件またはアプリケーション条件がある場合にのみ使用する
無効	有効	サーバー証明書がキャッシュされていない場合、プローブは常に送信されます。	非推奨

TLS 適応型サーバーのアイデンティティプローブ設定（復号ポリシー）	TLS 1.3 サーバーアイデンティティ検出設定（アクセス コントロール ポリシー）	結果	推奨される状況
無効	無効	プローブは送信されません。	実用性は非常に限定される。トラフィックを復号せず、アクセスコントロールルールでアプリケーション条件またはURL 条件を使用しない場合にのみ使用する

（注） キャッシュされた TLS サーバーの証明書は、特定の Firewall Threat Defense のすべての Snort インスタンスで利用できます。キャッシュはCLI コマンドでクリアでき、デバイスの再起動時に自動的にクリアされます。

参照

詳細については、secure.cisco.com で TLS サーバーアイデンティティ検出の説明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。