Decryption rulesとポリシーの例

この章は、このガイドで説明されている概念に基づいて作成されており、ベストプラクティスおよび推奨事項に従う decryption rules を使用した SSL ポリシーの特定の例を提供します。この例を実際の状況に当てはめ、組織のニーズに合わせて調整してください。

要約すると、次のようになります。

- 信頼できるトラフィック（圧縮された大規模なサーバーバックアップの転送など）の場合は、事前フィルタ処理とフローオフロードを使用して、検査を完全にバイパスします。
- 特定の IP アドレスに適用されるものなど、迅速に評価できるdecryption rulesを、「最初」に配置します。
- 処理（[復号-再署名（Decrypt - Resign）]）を必要とする decryption rules と、安全ではないプロトコルバージョンおよび暗号スイートをブロックするルールを「最後」に配置します。

Decryption rule 例

このセクションでは、decryption rule 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。

詳細については、次の項を参照してください。

復号ポリシーウィザードの実行

このタスクでは、アウトバウンドトラフィックを保護するために復号ポリシーウィザードを実行する方法について説明します。このポリシーには、4 つのルールが含まれています。

1. TLS/SSL ピンニングを使用している可能性が高いため、復号できないことがわかっている識別名を [復号しない（Do Not Decrypt）] ルール。
2. コンテンツに基づいて機密として分類される URL カテゴリ（医療や金融など）を [復号しない（Do Not Decrypt）] ルール。
3. TLS/SSL ピンニングを使用している可能性が高いため、復号できないことがわかっているアプリケーションを [復号しない（Do Not Decrypt）] ルール。
4. [IntCA] という名前の認証局オブジェクトを使用して残りのトラフィックを複合する [復号 - 再署名（Decrypt - Resign）] ルール。

ルールは必要に応じて編集できます。手動で以下を追加することもできます。

- トラフィックをモニターし、今後ブロックする必要があるかどうかを判断するための [復号 - 再署名（Decrypt - Resign）] ルール。
- 他のタイプのトラフィックを [復号しない（Do Not Decrypt）] ルール。
- 不正な証明書と安全でない暗号スイートの [ブロック（Block）] または [リセットしてブロック（Block With Reset）] ルール。

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。

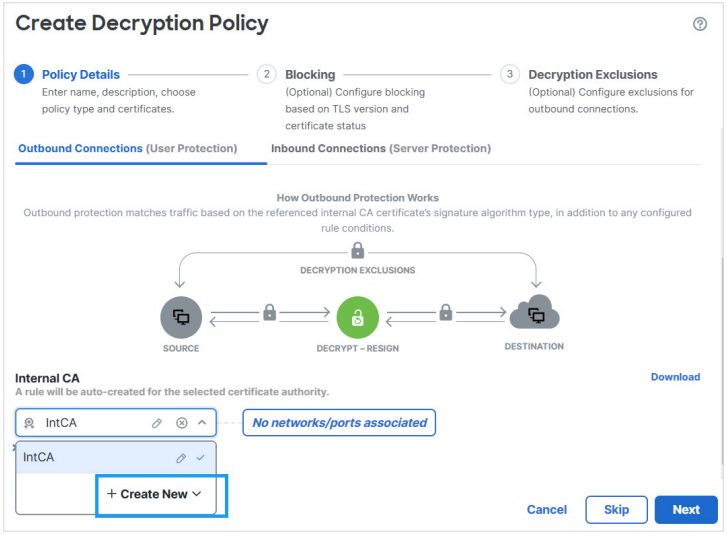
ステップ 3 [復号ポリシーの作成（Create Decryption Policy）] をクリックします。

ステップ 4 復号ポリシーの [名前（Name）] を入力し、オプションで [説明（Description）] を入力します。

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

ステップ 6 [内部CA（Internal CA）] リストから、内部認証局オブジェクトの名前をクリックするか、[新規作成（Create New）] をクリックしてアップロードまたは生成します。

次の図は例を示しています。



内部認証局オブジェクトの作成またはアップロードの詳細については、次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 のアップロード
- アウトバウンド保護のための内部 CA の生成

ステップ 7 （オプション）送信元ネットワークと接続先ネットワークへのトラフィックを制限するには、[ネットワークとポートを割り当てる場合はクリック（Click to assign networks and ports）] をクリックします。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 「復号ポリシー の除外」の説明に従って、ウィザードを完了します。

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。

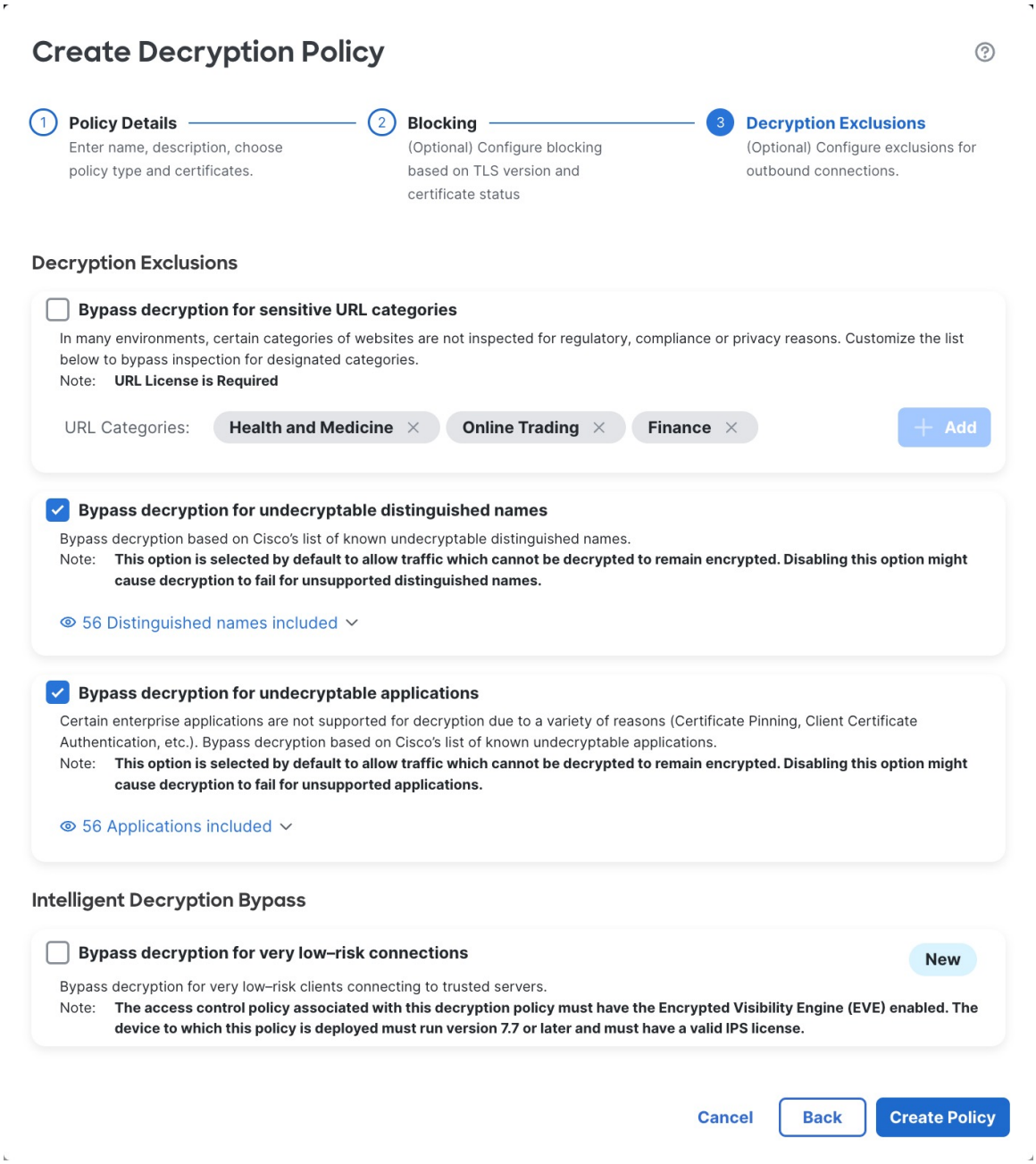
- アウトバウンド接続保護を使用した復号ポリシー の作成
- 詳細については、アウトバウンド接続保護を使用した復号ポリシーの作成を参照してください。

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。

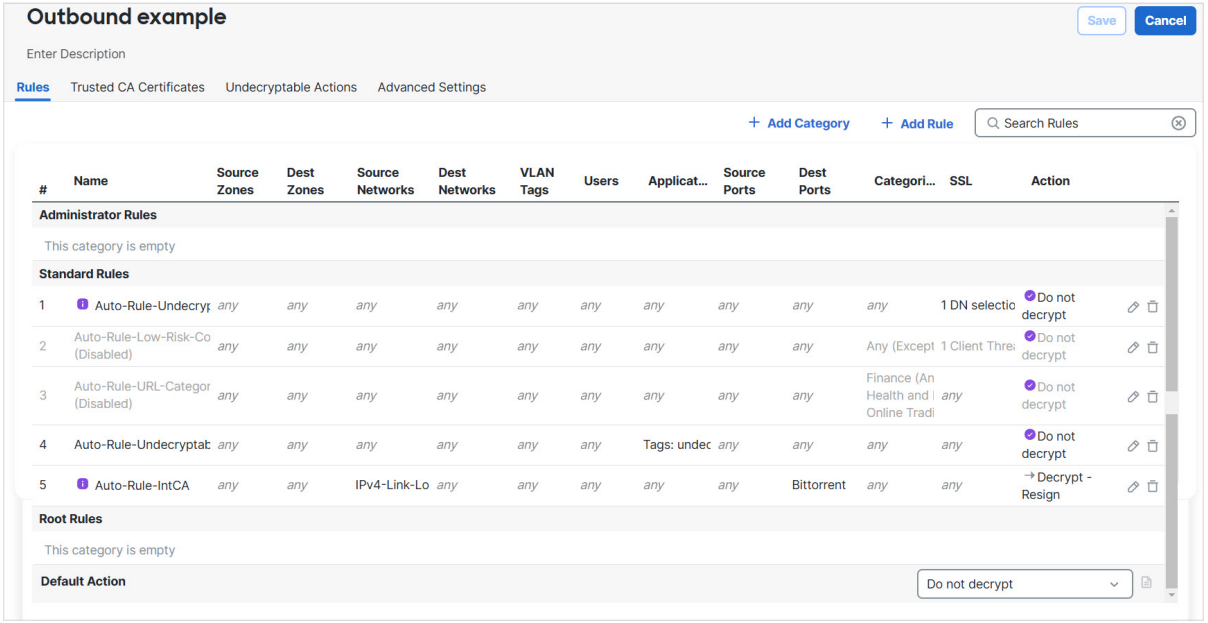
項目	説明
復号不能なアプリケーションの復号のバイパス（Bypass decryption for undecryptable applications）	証明書の再署名によって接続が失敗する可能性があるためトラフィックを復号しない場合は、このボックスをオンにします。 通常、この動作は 証明書のピン留めに関連付けられています。この操作については で説明されています。TLS/SSL 証明書のピン留めのガイドライン 復号できないアプリケーションは、脆弱性データベース（VDB）で自動的に更新されます。すべてのアプリケーションのリストは、Cisco Secure Firewall アプリケーションディ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。
[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。

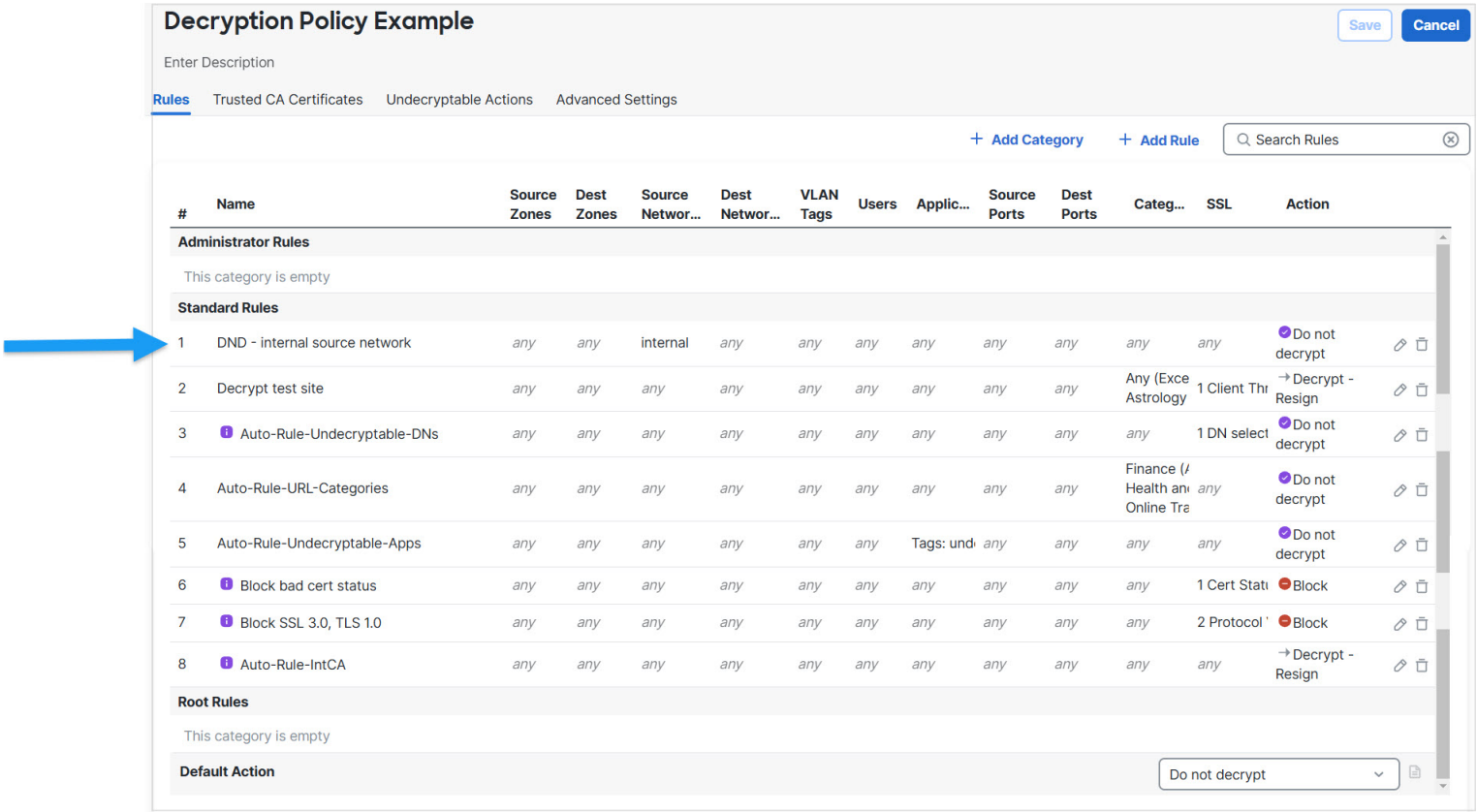
次のタスク

- 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
- *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
- 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。

最初の手動復号しないルール：特定のトラフィック

例の最初の decryption rule では、内部ネットワーク（**internal** 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。

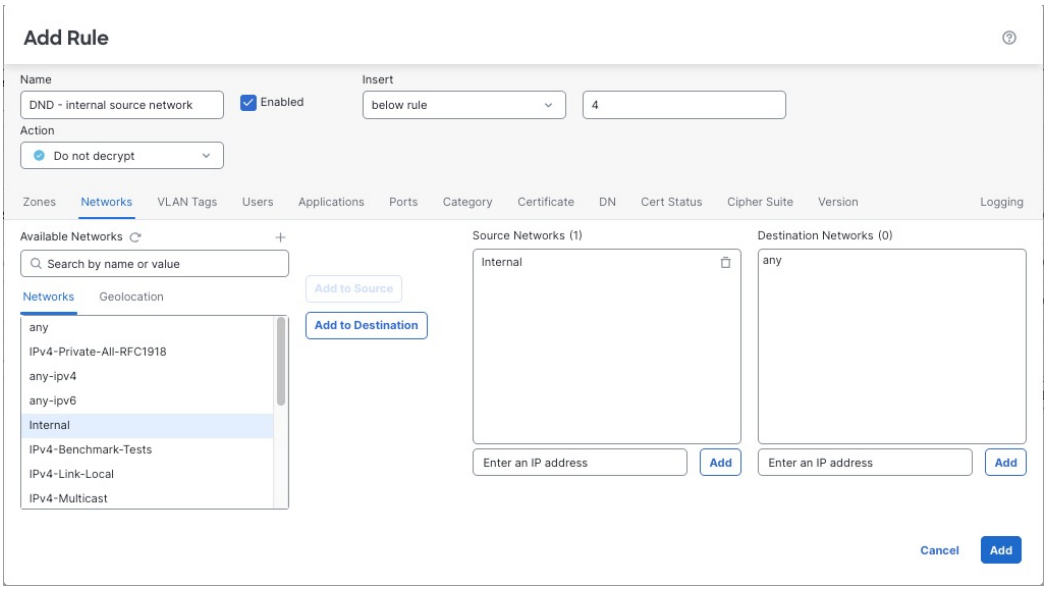
復号ポリシーウィザードを実行した後、ポリシーを編集して次のルールを追加します。ルールのリストの一番上にドラッグして、最初に評価されるようにします。



（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。

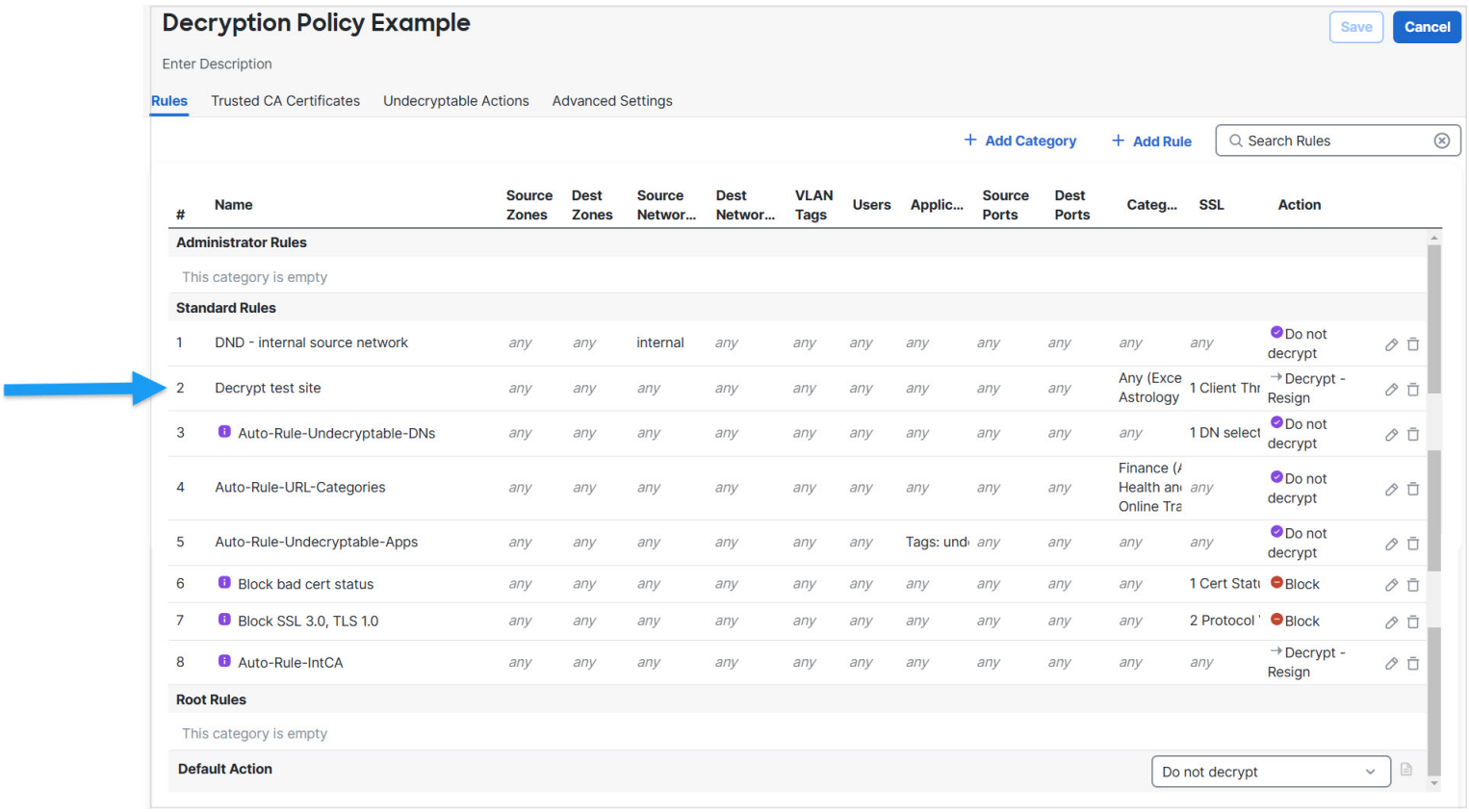
ルールの詳細：



次の手動ルール：特定の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。

復号ポリシーウィザードを実行した後、ポリシーを編集して次のルールを追加します。ルールのリストの 2 番目の位置にドラッグします。

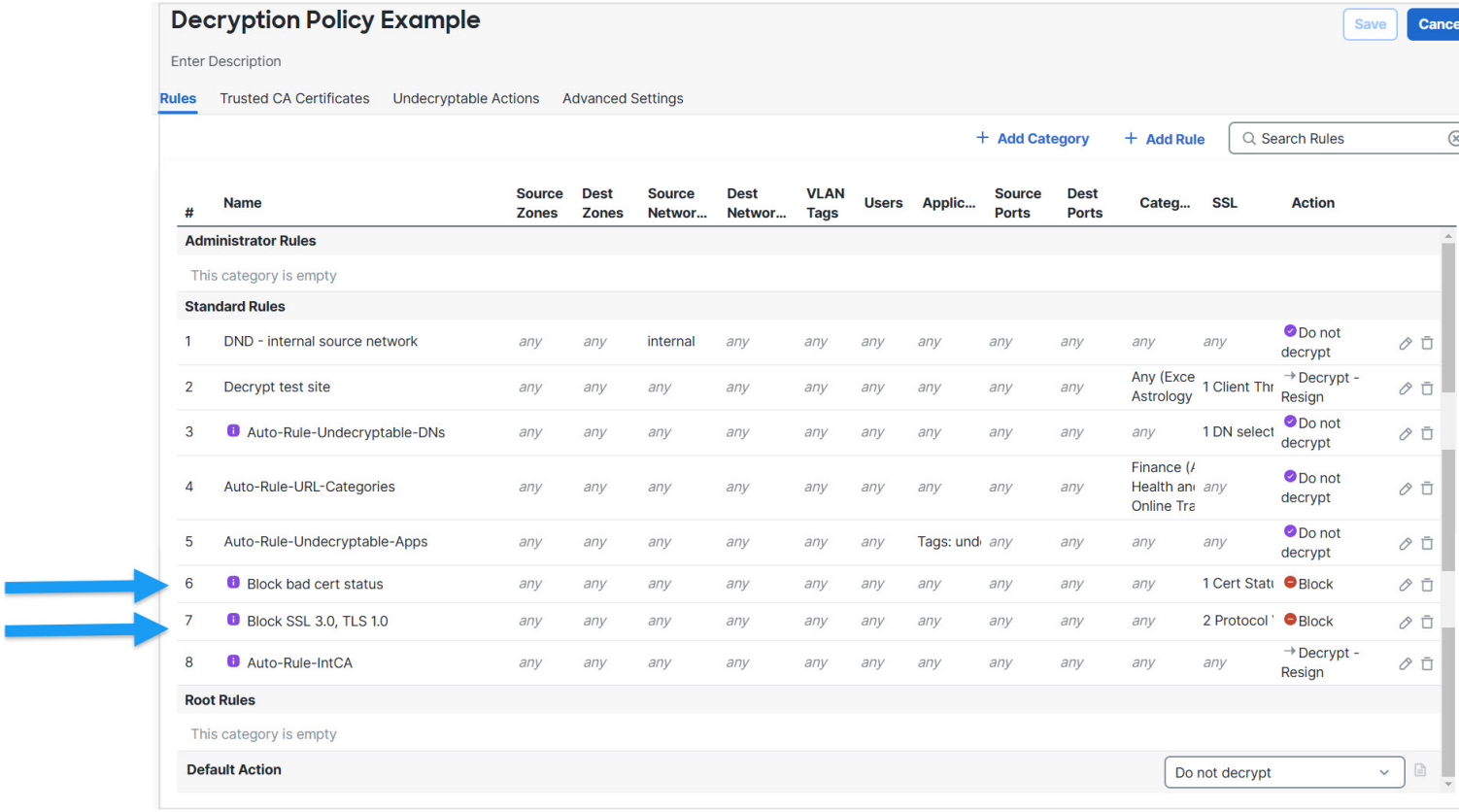


ルールの詳細：

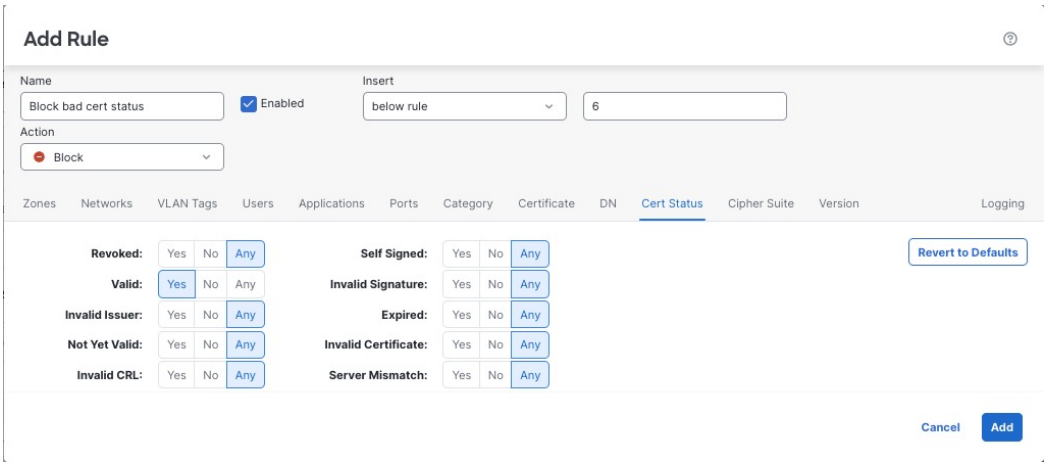
最後の手動Decryption rules：証明書とプロトコルバージョンをブロックまたは監視する

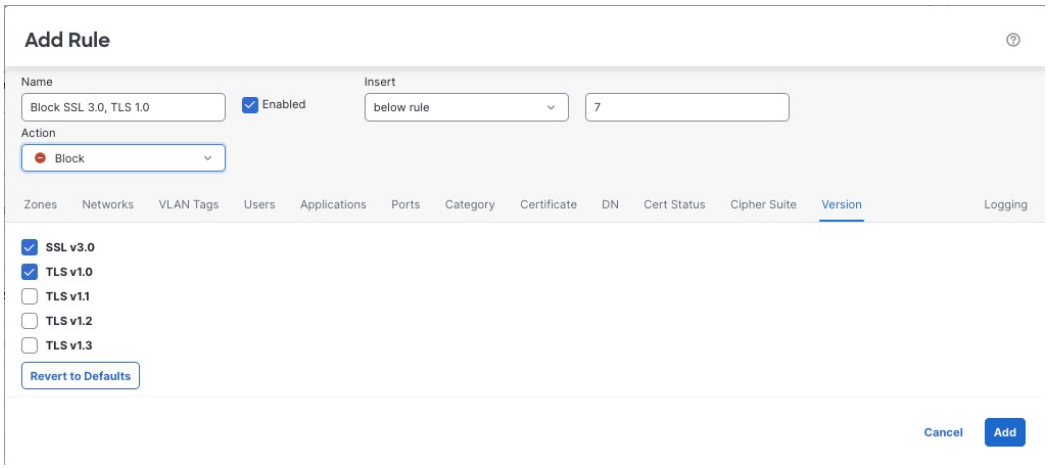
最後の decryption rulesは、最も具体的で最も処理が必要なルールのため、不正な証明書と安全でないプロトコルバージョンを監視またはブロックするルールです。

復号ポリシーウィザードを実行した後、ポリシーを編集して次のルールを追加します。それらを [復号 - 再署名（Decrypt - Resign）] ルールの前の位置にドラッグします。


Decryption Policy Example
Save
Cance
Enter Description
Rules
Trusted CA Certificates
Undecryptable Actions
Advanced Settings
+ Add Category
+ Add Rule
Search Rules
Name Source Zones Dest Zones Source Networ... Dest Networ... VLAN Tags Users Applic... Source Ports Dest Ports Categ... SSL Action
Administrator Rules
This category is empty
Standard Rules
1 DND - internal source network any any internal any any any any any any any any Do not decrypt
2 Decrypt test site any any any any any any any any any Any (Exce Astrology 1 Client Thr Decrypt - Resign
3 Auto-Rule-Undecryptable-DNs any any any any any any any any any any 1 DN select Do not decrypt
4 Auto-Rule-URL-Categories any any any any any any any any any Finance (Health an Online Tra any Do not decrypt
5 Auto-Rule-Undecryptable-Apps any any any any any any Tags: und any any any any Do not decrypt
6 Block bad cert status any any any any any any any any any any 1 Cert Stat Block
7 Block SSL 3.0, TLS 1.0 any any any any any any any any any any 2 Protocol Block
8 Auto-Rule-IntCA any any any any any any any any any any any Decrypt - Resign
Root Rules
This category is empty
Default Action
Do not decrypt

ルールの詳細：


Add Rule
Name
Block bad cert status
Enabled
Insert
below rule
6
Action
Block
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging
Revoked: Yes No Any
Valid: Yes No Any
Invalid Issuer: Yes No Any
Not Yet Valid: Yes No Any
Invalid CRL: Yes No Any
Self Signed: Yes No Any
Invalid Signature: Yes No Any
Expired: Yes No Any
Invalid Certificate: Yes No Any
Server Mismatch: Yes No Any
Revert to Defaults
Cancel
Add



例：証明書ステータスを監視またはブロックする Decryption rule

最後の decryption rules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。

重要 [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。**[暗号スイート（Cipher Suite）]** および **[バージョン（Version）]** を、**[復号 - 再署名（Decrypt - Resign）]** または **[復号 - 既知のキー（Decrypt - Known Key）]** ルールアクションと併用しないでください。ルールのこれらの条件を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 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 の横にある **Edit** (✎) をクリックします。

ステップ 4 decryption rule の横にある **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 [追加（Add）] 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 Decryption rule

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。

- decryption rule 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、decryption policy 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。

重要 [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。**[暗号スイート（Cipher Suite）]** および **[バージョン（Version）]** を、**[復号 - 再署名（Decrypt - Resign）]** または **[復号 - 既知のキー（Decrypt - Known Key）]** ルールアクションと併用しないでください。ルールのこれらの条件を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 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 の横にある **Edit** (✎) をクリックします。

ステップ 4 decryption rule の横にある **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。

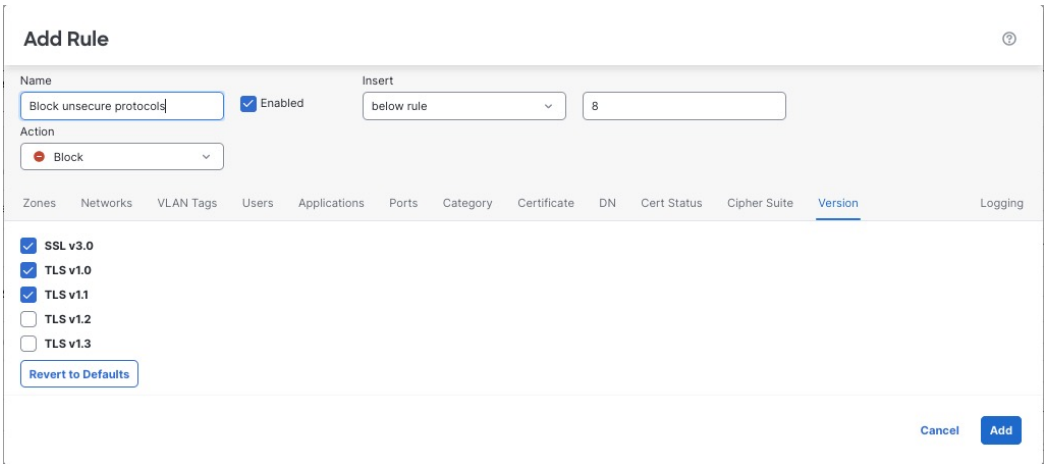
ステップ 6 [ルールの追加（Add Rule）] ダイアログボックスの [名前（Name）] フィールドに、ルールの名前を入力します。

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 **[追加（Add）]** をクリックします。

オプションの例：証明書識別名の監視またはブロックのマニュアル Decryption rule

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、「*Cisco Secure Firewall Management Center* デバイス設定ガイド」の識別名（DN）ルールの条件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 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 の横にある **Edit** (✎) をクリックします。

ステップ 4 decryption rule の横にある **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。入力を開始するとリストが更新され、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 ドロップでリストに追加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。[Subject DNs] または [Issuer DNs] リストの下にある [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 [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。

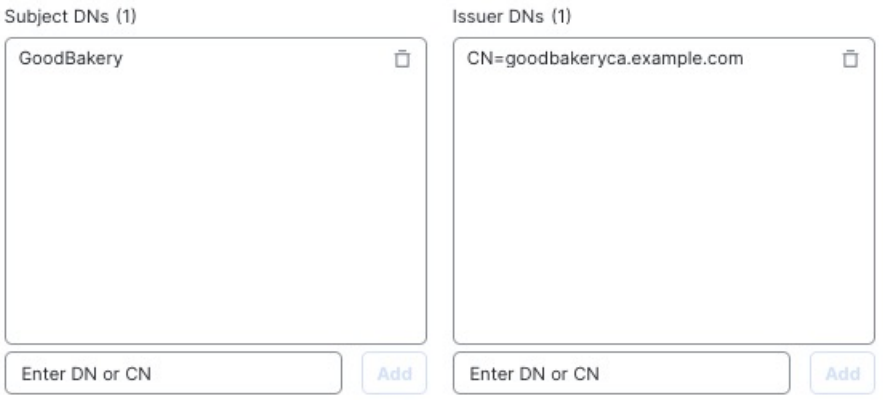
ステップ 13 ルールを追加するか、編集を続けます。

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 [追加（Add）] 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。



Decryption policy とアクセス コントロール ポリシーの関連付けと詳細設定

このタスクでは、decryption policy をアクセス コントロール ポリシーに関連付ける方法と、アクセス コントロール ポリシーの推奨される詳細設定を設定する方法について説明します。

decryption policy をシステムで使用するには、必ずアクセス コントロール ポリシーに関連付けます。

始める前に

このガイドの説明に従って、サンプルの復号ポリシーを作成してください。

decryption policy の詳細オプションについて詳しくは、復号ポリシー 詳細オプション.

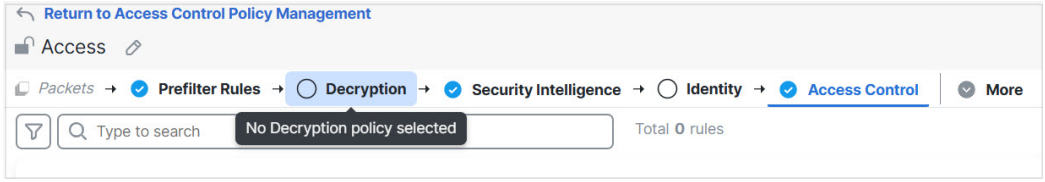
手順

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。

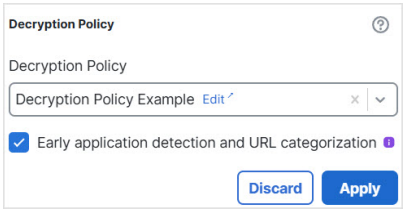
ステップ 2 **Policies** > **Access Control heading** > **Access Control** をクリックします。

ステップ 3 新しいアクセス コントロール ポリシーを作成するか、[**Edit** (✎)] をクリックして既存のポリシーを編集します。

ステップ 4 次の図に示すように、[復号（Decryption）] をクリックします。

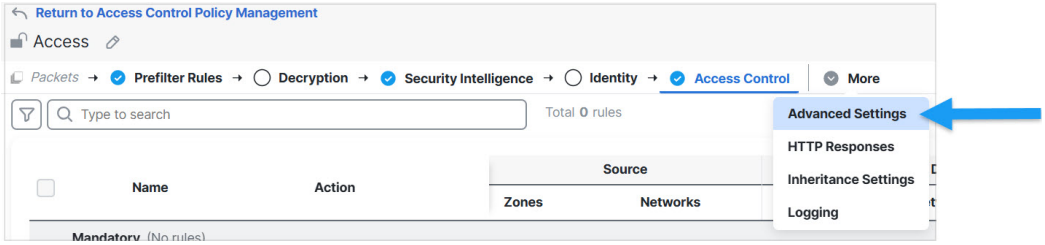


ステップ 5 次の図に示すように、リストで復号ポリシーの名前をクリックし、さらに[早期アプリケーション検出とURL分類（Early application detection and URL categorization）] をオンにします。



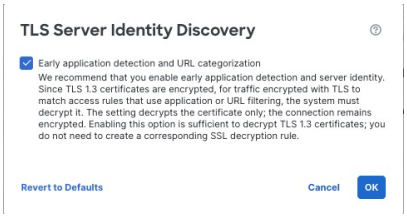
ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 次の図に示すように、**[詳細（More）]** > **[詳細設定（Advanced Settings）]** をクリックします。



ステップ 8 [TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）] の横の [**Edit** (✎)] をクリックします。

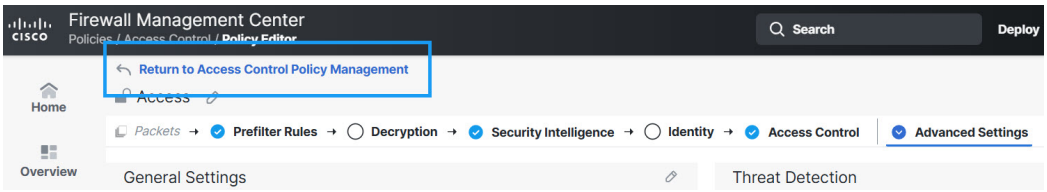
ステップ 9 次の図に示すように、チェックボックスをオンにします。



ステップ 10 [OK] をクリックします。

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。

ステップ 12 次の図に示すように、ページの上部にある [アクセスコントロールポリシー管理に戻る（Return to Access Control Policy Management）] をクリックします。



ステップ 13 [**Edit** (✎)] をクリックして、アクセスコントロールルールを編集します。

ステップ 14 ページの下部で、デフォルトアクションの横にある [ ] （デフォルトのロギングおよびインスペクション（Default Logging and Inspection））をクリックします。

ステップ 15 [接続開始時にロギング（Log at starting of connection）] と、選択したその他のオプションをオンにします。

詳細については、『*Cisco Secure Firewall Management Center Device Configuration Guide*』の アクセス コントロール ポリシーのロギング設定「Logging Settings for Access Control Policies」[英語] を参照してください。

ステップ 16 [Apply] をクリックします。

ステップ 17 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

- 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
- *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
- 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。

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

Decryption rule の設定

decryption rules に推奨されるベストプラクティス設定の設定方法。

Decryption rules：[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 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 の横にある **Edit** (✎) をクリックします。

ステップ 4 decryption rule の横にある **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。