



## 復号ルールとポリシーの例

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復号ルールを使用した 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、迅速に評価できる復号ルールを、「最初」に配置します。
- 処理（[復号-再署名（Decrypt - Resign）]）を必要とする復号ルールと、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。
- [復号ルール ベスト プラクティス（1 ページ）](#)
- [復号ポリシーのウォークスルー（5 ページ）](#)

## 復号ルール ベスト プラクティス

この章では、復号ルールを持つ 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 방법으로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

### SSL Policy Example

Enter Description

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
<b>Administrator Rules</b>													
This category is empty													
<b>Standard Rules</b>													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Do not decrypt
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any any		Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Low	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Pho	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ui any		Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status se	Block
7	Block SSLv3, TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
<b>Root Rules</b>													
This category is empty													
Default Action												Do not decrypt	

## 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。

#### 関連トピック

[大規模フローのオフロード](#)

[プレフィルタリングとアクセス コントロール](#)

[Fastpath プレフィルタリングのベストプラクティス](#)

## 【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。いずれかの復号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。

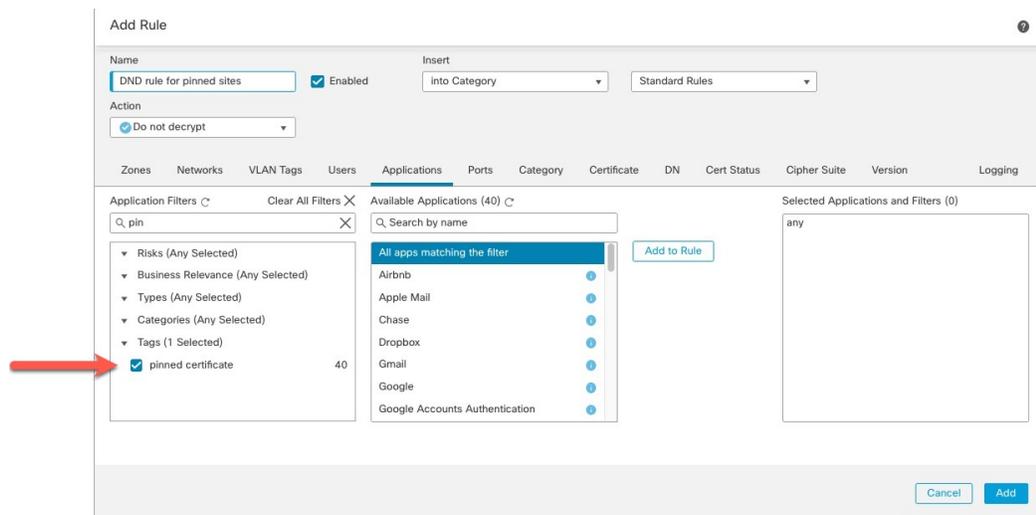
証明書のピン留めの詳細については、[TLS/SSL のピンングについて](#)を参照してください。

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
- **ピン留めされた証明書**のアプリケーションフィルタ

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、復号ルールの下部に【復号しない (Do Not Decrypt)】ルールを設定することを推奨します。

**ピン留めされた証明書**のアプリケーションフィルタの設定例を次に示します。



## 【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。復号ルール

### 【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、ピンニングまたは証明書ピン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)】アクションで復号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、[Cisco Secure Firewall Management Center デバイス構成ガイド「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 復号ルール

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 復号ルール

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

## 復号ポリシーのウォークスルー

この章では、ベストプラクティスを採用するルールを使用する復号ポリシーを作成する方法について、段階的な説明とウォークスルーを示します。復号ポリシーのプレビューに続いてベストプラクティスの概要を示し、最後にポリシーのルールについて説明します。

以下は、この章で説明する復号ポリシーです。

SSL Policy Example Save Cancel

Enter Description

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
<b>Administrator Rules</b>													
This category is empty													
<b>Standard Rules</b>													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Do not decrypt
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any any		→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Low	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Pho	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Ui any		→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status st	Block
7	Block SSLv3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
<b>Root Rules</b>													
This category is empty													
Default Action												Do not decrypt	

詳細については、次の項を参照してください。

#### 関連トピック

[推奨ポリシーとルールの設定 \(6 ページ\)](#)

[プレフィルタするトラフィック \(11 ページ\)](#)

[最初の復号ルール：特定のトラフィックを復号しない \(11 ページ\)](#)

[次の復号ルール：特定のテストトラフィックを復号する \(12 ページ\)](#)

[カテゴリの \[復号-再署名 \(Decrypt - Resign\)\] ルールの作成 \(15 ページ\)](#)

[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 \(13 ページ\)](#)

[最後の復号ルール：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 \(16 ページ\)](#)

## 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。

- 復号ポリシー：
  - 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。
- ポリシーの詳細設定で TLS 1.3 復号を有効にします。
- 復号ルール: [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:
  - 復号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、復号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

[復号ポリシーの設定](#) (7 ページ)

[復号ルールの設定](#) (24 ページ)

[アクセスコントロールポリシーの設定](#) (9 ページ)

## 復号ポリシーの設定

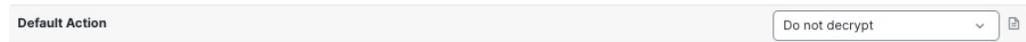
復号ポリシーに推奨される次のベストプラクティス設定の設定方法。

- 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。
- ポリシーの詳細設定で TLS 1.3 復号を有効にします。

#### 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** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [復号 (Decryption)] をクリックします。
- ステップ 3** 復号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。

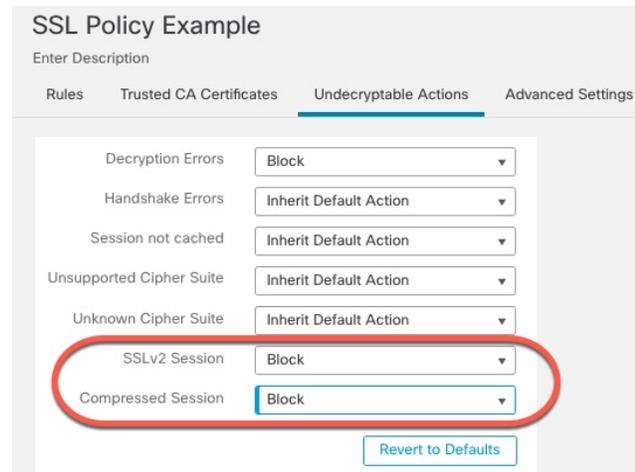


- ステップ5 行の最後で、[ロギング (Logging)] ( ) をクリックします。
- ステップ6 [接続の終了時にロギングする (Log at End of Connection)] チェックボックスをオンにします。
- ステップ7 [OK] をクリックします。
- ステップ8 [保存 (Save)] をクリックします。
- ステップ9 [復号不可のアクション (Undecryptable Actions)] タブをクリックします。
- ステップ10 [SSLv2セッション (SSLv2 Session)] と [圧縮セッション (Compressed Session)] のアクションは [ブロック (Block)] に設定することを推奨します。

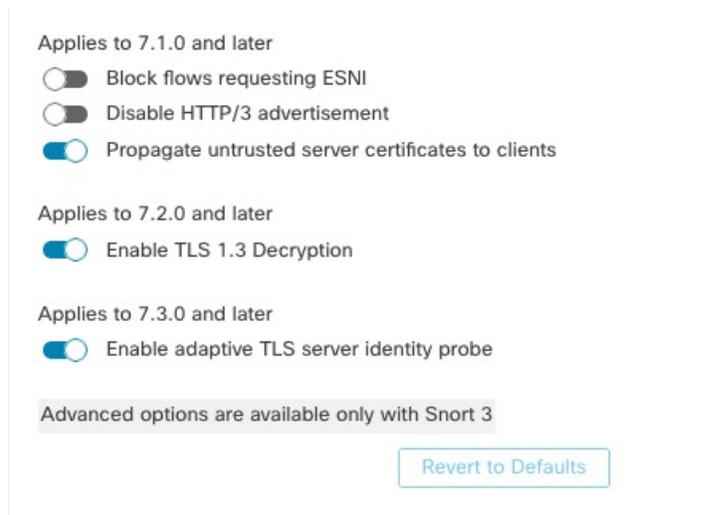
ネットワークで SSLv2 を許可しないでください。圧縮された TLS/SSL トラフィックはサポートされていないためブロックする必要があります。

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 [詳細設定 (Advanced Settings)] タブページをクリックします。
- ステップ12 [TLS 1.3復号の有効化 (Enable TLS 1.3 Decryption)] チェックボックスをオンにします。他のオプションの詳細については、[復号ポリシーの詳細オプション](#)セクションの「AdvancedDecryption」オプションのセクションを参照してください。



**ステップ 13** 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

[復号ルール の設定 \(24 ページ\)](#) の説明に従い、復号ルール 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：

- 復号ポリシー 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、復号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

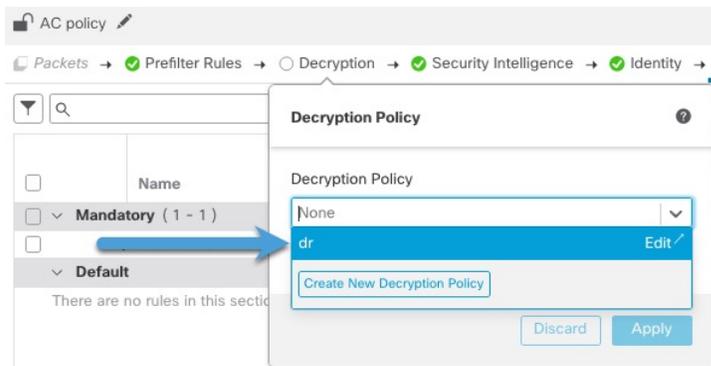
**ステップ 1** まだ Secure Firewall Management Center にログインしていない場合は、ログインします。

**ステップ 2** [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

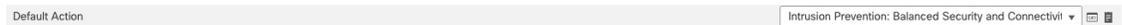
**ステップ 4** (復号ポリシーがまだ設定されていない場合は、後で設定できます)。

- 次の図に示すように、ページの上にある [復号 (Decryption)] リンクをクリックします。



- b) リストから、有効にする復号ポリシーの名前をクリックします
- c) [Apply] 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

[復号ルール例 \(10 ページ\)](#) を参照してください。

## 復号ルール例

このセクションでは、復号ルールの例を示し、シスコのベストプラクティスについて説明します。

詳細については、次の項を参照してください。

### 関連トピック

[プレフィルタするトラフィック \(11 ページ\)](#)

[最初の復号ルール：特定のトラフィックを復号しない \(11 ページ\)](#)

[次の復号ルール：特定のテストトラフィックを復号する \(12 ページ\)](#)

[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 \(13 ページ\)](#)

[カテゴリの \[復号-再署名 \(Decrypt - Resign\)\] ルールの作成 \(15 ページ\)](#)

最後の復号ルール：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 (16 ページ)

## 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 [https://en.wikipedia.org/wiki/Elephant\\_flow](https://en.wikipedia.org/wiki/Elephant_flow)

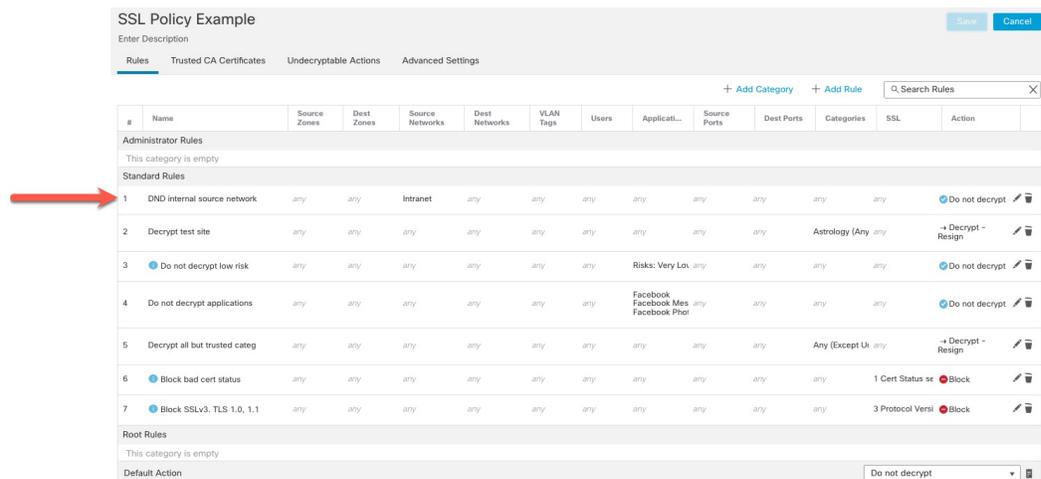
### 関連トピック

[プレフィルタリングとアクセスコントロール](#)

[Fastpath プレフィルタリングのベストプラクティス](#)

## 最初の復号ルール：特定のトラフィックを復号しない

例の最初の復号ルールでは、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。



#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Do not decrypt
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any any	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Low	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Un	any	→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status ss	Block
7	Block SSLv3, TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
Root Rules													
This category is empty													
Default Action													
Do not decrypt													

## 次の復号ルール：特定のテストトラフィックを復号する



(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。

The screenshot shows the configuration for a rule named "DND internal source network". The rule is enabled and set to "Do not decrypt". The source network is "Intranet" and the destination network is "any". The interface includes tabs for Zones, Networks, VLAN Tags, Users, Applications, Ports, Category, Certificate, DN, Cert Status, Cipher Suite, Version, and Logging. The "Available Networks" list includes "any", "IPv4-Private-All-RFC1918", "any-ipv4", "any-ipv6", "defaultgateway", "insidesubnet", "Intranet", and "IPv4-Benchmark-Tests".

## 次の復号ルール：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。

SSL Policy Example

Enter Description

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

+ Add Category + Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Do not decrypt
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any any		Do not decrypt
3	Do not decrypt low risk	any	any	any	any	any	any	any	Risks: Very Low	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phor	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except U any		Do not decrypt
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status st	Block
7	Block SSLv3, TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
Root Rules													
This category is empty													
Default Action													
Do not decrypt													

ルールの詳細：

Editing Rule - Decrypt test site

Name: Decrypt test site  Enabled [Move](#)

Action: Decrypt - Resign with IntCA  Replace Key Only

Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Categories

- Any (Except Uncategorized)
- Uncategorized
- Adult
- Advertisements
- Alcohol
- Animals and Pets
- Arts
- Astrology

Reputations

- Any
- 5 - Trusted
- 4 - Favorable
- 3 - Neutral
- 2 - Questionable
- 1 - Untrusted

Apply to unknown reputation

Selected Categories (1)

- Astrology (Any reputation)

Cancel Save

## 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。

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

SSL Policy Example Save Cancel

Enter Description

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Do not decrypt
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any	any	Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Low	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Uk	any	Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status st	Block
7	Block SSLv3, TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi
Root Rules													
This category is empty													
Default Action													
													Do not decrypt

ルールの詳細:

Editing Rule - Do not decrypt low risk ?

Name  
Do not decrypt low risk  Enabled [Move](#)

Action  
Do not decrypt

Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Application Filters  Clear All Filters Available Applications (1483)

Application Filters	Available Applications (1483)	Selected Applications and Filters (1)
<ul style="list-style-type: none"> <li>▼ Risks (Any Selected) <ul style="list-style-type: none"> <li><input type="checkbox"/> Very Low 538</li> <li><input type="checkbox"/> Low 454</li> <li><input type="checkbox"/> Medium 282</li> <li><input type="checkbox"/> High 139</li> <li><input type="checkbox"/> Very High 70</li> <li>▼ Business Relevance (Any Selected) <ul style="list-style-type: none"> <li><input type="checkbox"/> Very Low 580</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>050plus</li> <li>1&amp;1 Internet</li> <li>1-800-Flowers</li> <li>1000mercis</li> <li>12306.cn</li> <li>123Movies</li> <li>126.com</li> <li>17173.com</li> </ul>	<p>Filters</p> <p>Risks:Very Low, Low</p>

[< < Viewing 1-100 of 1483 > >]

Cancel Save

### 関連トピック

- [アプリケーション制御の設定のベストプラクティス](#)
- [アプリケーション制御に関する推奨事項](#)

## 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復号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 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 内部認証局 (CA) を Secure Firewall 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) ]>[復号 (Decryption) ] 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。

## 関連トピック

[内部認証局オブジェクト](#)

## 最後の復号ルール：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

最後の復号ルールは、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。

SSL Policy Example

Enter Description

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND internal source network	any	any	Intranet	any	any	any	any	any	any	any	any	Do not decrypt
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any any	any	→ Decrypt - Resign
3	Do not decrypt low risk	any	any	any	any	any	any	Risks: Very Lo...	any	any	any	any	Do not decrypt
4	Do not decrypt applications	any	any	any	any	any	any	Facebook Facebook Mes Facebook Phot	any	any	any	any	Do not decrypt
5	Decrypt all but trusted categ	any	any	any	any	any	any	any	any	any	Any (Except Uk any	any	→ Decrypt - Resign
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status s4	Block
7	Block SSLV3. TLS 1.0, 1.1	any	any	any	any	any	any	any	any	any	any	3 Protocol Versi	Block
Root Rules													
This category is empty													
Default Action													
													Do not decrypt

ルールの詳細：

Editing Rule - Block bad cert status

Name: Block bad cert status  Enabled [Move](#)

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](#) [Save](#)

## 例：証明書ステータスを監視またはブロックする 復号ルール

## 関連トピック

例：証明書ステータスを監視またはブロックする 復号ルール (18 ページ)

例：プロトコルバージョンを監視またはブロックする 復号ルール (20 ページ)

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 復号ルール (22 ページ)

## 例：証明書ステータスを監視またはブロックする 復号ルール

最後の復号ルールは、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 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 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [復号 (Decryption)] 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 復号ルールの横にある [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。

Revoked:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any	Self Signed:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any
Valid:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Any	Invalid Signature:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any
Invalid Issuer:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any	Expired:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any
Not Yet Valid:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any	Invalid Certificate:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any
Invalid CRL:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any	Server Mismatch:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Any

## 例：プロトコルバージョンを監視またはブロックする 復号ルール

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。

Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	Yes	No	Any	Server Mismatch:	Yes	No	Any

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。

Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	Yes	No	Any	Server Mismatch:	Yes	No	Any

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。

Revoked:	Yes	No	Any	Self Signed:	Yes	No	Any
Valid:	Yes	No	Any	Invalid Signature:	Yes	No	Any
Invalid Issuer:	Yes	No	Any	Expired:	Yes	No	Any
Not Yet Valid:	Yes	No	Any	Invalid Certificate:	Yes	No	Any
Invalid CRL:	Yes	No	Any	Server Mismatch:	Yes	No	Any

## 例：プロトコルバージョンを監視またはブロックする 復号ルール

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。

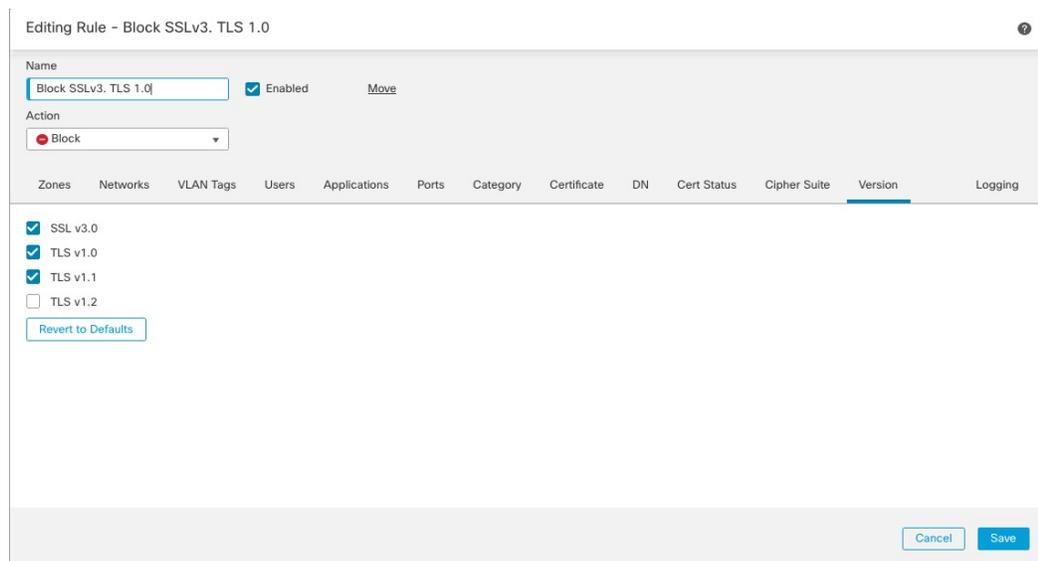


(注) [暗号スイート (Cipher Suite)]と[バージョン (Version)]のルール条件は、[ブロック (Block)]または[リセットしてブロック (Block with reset)]のルールアクションが使用されているルールでのみ使用します。これらの条件をルールで他のルールアクションとともに使用すると、システムのClientHello処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

#### 手順

- ステップ 1** まだ 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** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [復号 (Decryption)] 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** 復号ルールの横にある [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 復号ルール

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。識別名 (DN) のルール条件の「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 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** [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [復号 (Decryption) ] 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** 復号ルール 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 DN)] 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 DN)] 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 DN)] 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 DN)] または [発行元 DN (Issuer DN)] 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 DN)] 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。

Subject DNs (1)	Issuer DNs (1)
<div style="border: 1px solid gray; padding: 5px;">           GoodBakery <span style="float: right;">🗑️</span> </div>	<div style="border: 1px solid gray; padding: 5px;">           CN=goodca.example.com <span style="float: right;">🗑️</span> </div>
<input type="text" value="Enter DN or CN"/> <input type="button" value="Add"/>	<input type="text" value="Enter DN or CN"/> <input type="button" value="Add"/>

## 復号ルール の設定

復号ルール に推奨されるベストプラクティス設定の設定方法。

復号ルール : [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 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 [ポリシー (Policies) ] > [アクセスコントロール (Access Control) ] > [復号 (Decryption) ] 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 復号ルール 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。