# TLS/SSL ルールを使用した復号の調整

次のトピックでは、TLS/SSL ルール条件を設定する方法の概要を示します。



## TLS/SSL ルール条件の概要

デバイスで検査されるすべての暗号化トラフィックには、基本的な TLS/SSL ルールに基づいたアクションが適用されます。暗号化トラフィックをより詳細に復号化および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 TLS/SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックに TLS/SSL ルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。

（注） トラフィックがルールに一致すると、デバイスは設定されたルールアクションをトラフィックに適用します。ログの記録が指定されている場合、接続が終了した時点でトラフィックに関するログが記録されます。

各ルール条件には、照合するトラフィックのプロパティを 1 つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティ ゾーン、IP アドレスおよびポート、送信元または宛先の国、送信元または宛先の VLAN などのトラフィック フロー。
- 検出された IP アドレスに関連付けられたユーザ。
- トラフィックで検出されたアプリケーションなどのトラフィック ペイロード。
- 接続の暗号化に使用された TLS/SSL プロトコル バージョン、暗号スイート、サーバ証明書などの接続暗号化。
- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション。

関連トピック



# サーバ証明書ベースの TLS/SSL ルール条件

TLS/SSL ルールでは、サーバ証明書の特性に基づいて暗号化トラフックを処理および復号できます。TLS/SSL ルールは、以下のサーバ証明書属性に基づいて設定することができます。

- 識別名条件を設定すると、証明書所有者またはサーバ証明書の発行元 CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。
- TLS/SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。
- TLS/SSL ルールの証明書ステータス条件では、トラフィックの暗号化に使用されたサーバ証明書のステータスに基づいて暗号化されたトラフィックを処理して、証明書が有効か、失効しているか、期限切れか、まだ有効でないか、自己署名済みか、信頼できる CA によって署名済みか、証明書失効リスト（CRL）が有効かどうか、証明書のサーバ名指定（SNI）が要求内のサーバと一致するかどうかなどの検査を行うことができます。
- TLS/SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。
- TLS/SSL ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出する場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに

追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

# 証明書の識別名の TLS/SSL ルール条件

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。

（注） [復号 - 既知のキー（Decrypt - Known Key）] アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われています。

複数のサブジェクトおよび発行元の識別名との一致を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは1つの共通名または識別名だけです。

識別名を手動で追加する場合、共通名属性（**CN**）を含めることができます。`CN=` なしで共通名を追加すると、オブジェクトを保存する前に `CN=` が追加されます。

また、以降の属性ごとに1つずつ識別名をカンマで区切って追加することができます。たとえば、**C, CN, O, OU** というようにします。

1 つの識別名条件で、[サブジェクト DN（Subject DNs）] リストおよび [発行元 DN（Issuer DNs）] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

システム提供の識別名オブジェクト グループである Cisco-Undecryptable-Sites には、システムで復号できないトラフィックの Web サイトが含まれます。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号化を無効にしたりでき、これらのトラフィックの復号化に使用されるシステム リソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によってこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

システムが新しいサーバへの暗号化セッションを最初に検出したときは、DN データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは識別名条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

# 証明書の識別名による暗号化トラフィックの制御

| スマート ライセンス | 従来のライセンス | サポートされるデバイス数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | すべて（NGIPSvを除く） | いずれか（Any） | Admin/Access Admin/Network Admin |

**ステップ 1** SSL ルール エディタで、[DN] タブを選択します。

**ステップ 2** [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）] リストの上にある追加アイコン（）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、[Available DNs] リストの上にある [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 3** 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 [Select All] を選択します。

**ステップ 4** [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。

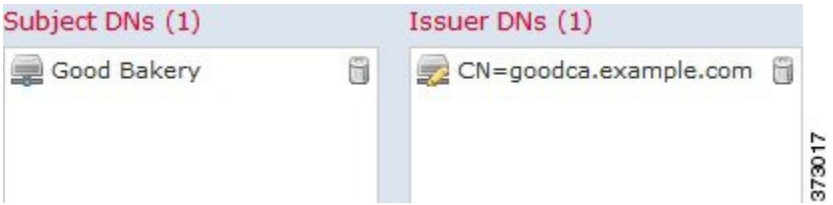
**ステップ 5** 手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。[Subject DNs] または [Issuer DNs] リストの下にある [Enter DN or CN] プロンプトをクリックし、共通名または識別名を入力して [Add] をクリックします。

**ステップ 6** ルールを追加するか、編集を続けます。

**例**

**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。



次の図は、badbakery.example.com および関連ドメインに対して発行された証明書およびbadca.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、再署名された証明書を使用して復号されます。


### 次のタスク

- 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。

### 関連トピック

識別名オブジェクト

# 証明書の TLS/SSL ルール条件

証明書ベースの TLS/SSL ルール条件を作成するときにサーバ証明書をアップロードしたり、再利用可能な外部証明書オブジェクトとして保存してサーバ証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [Available Certificates] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名に関する以下の特性に基づいて検索できます。

- 件名または発行元の共通名（CN）
- 件名または発行元の組織（O）
- 件名または発行元の部門（OU）

1 つの証明書のルール条件で複数の証明書に一致させることもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[Selected Certificates] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- **Decrypt - Known Key** アクションを選択した場合、証明書条件を設定することはできません。このアクションでは、トラフィック復号化用のサーバ証明書の選択が必要であり、トラフィックの照合はすでにこの証明書で行われることになります。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれ

かが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。

- システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

# 証明書による暗号化トラフィックの制御

| スマート ライセンス | 従来のライセンス | サポートされるデバイス数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | すべて（NGIPSv を除く） | いずれか（Any） | Admin/Access Admin/Network Admin |

**ステップ 1** SSL ルール エディタで、[証明書（Certificate）] タブを選択します。

**ステップ 2** [使用可能な証明書（Available Certificates）] で、追加するサーバ証明書を探します。

- ここで外部証明書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）、[使用可能な証明書（Available Certificates）] リストの上にある追加アイコン（）をクリックします。
- 追加する証明書オブジェクトおよびグループを検索するには、[Available Certificates] リストの上にある [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 3** 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 [Select All] を選択します。

**ステップ 4** [Add to Rule] 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 5** ルールを追加するか、編集を続けます。

### 次のタスク

- 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。

**関連トピック**

外部証明書オブジェクト

# 証明書ステータスの TLS/SSL ルール条件

証明書ステータスの TLS/SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

複数の証明書ステータスの有無を単一の証明書ステータスルール条件で照合するように選択できます（いずれか 1 つの基準に一致するだけで、その証明書はルールに一致します）。

このパラメータを設定するときは、復号ルールを設定するのか、ブロックルールを設定するのかを検討する必要があります。通常、ブロックルールでは[はい（Yes）]、復号ルールでは[いいえ（No）] をクリックします。次に例を示します。

- [復号 - 再署名（Decrypt - Resign）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書でのトラフィックを復号します。その動作を変更するには、[期限切れ（Expired）] で[いいえ（No）] をクリックし、期限切れの証明書を持つトラフィックが復号され、再署名されないようにします。
- [ブロック（Block）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書を持つトラフィックを許可します。その動作を変更するには、[期限切れ（Expired）] で[はい（Yes）] をクリックし、期限切れの証明書を持つトラフィックをブロックします。

次の表は、暗号化用のサーバ証明書のステータスを基準に、システムが暗号化トラフィックを評価する方法を示しています。

**表 *1*：証明書ステータスのルール条件の基準**

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| Revoked | ポリシーは、サーバ証明書を発行したCAを信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれています。 | ポリシーは、サーバ証明書を発行したCAを信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。 |
| Self-signed | 検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。 | 検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。 |

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| Valid | 以下のすべてを満たしています。<br>• ポリシーが証明書を発行した CA を信用できる。<br>• 署名は有効である。<br>• 発行元は有効である。<br>• ポリシーの信頼できる CA のいずれも証明書を失効させていません。<br>• 現在の日付が証明書の有効期間の開始日と終了日の範囲内にある。 | 以下の 1 つ以上を満たしています。<br>• 証明書を発行した CA をポリシーが信頼していない。<br>• 署名が無効である。<br>• 発行元が無効である。<br>• ポリシーの信用できる CA の 1 つが原因で証明書が失効している。<br>• 現在の日付が証明書の有効期間の開始日より前です。<br>• 現在の日付が証明書の有効期限の終了日より後です。 |
| Invalid signature | 証明書の内容に対して証明書の署名が適切に検証されません。 | 証明書の内容に対して証明書の署名が適切に検証されます。 |
| Invalid issuer | 発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。 | 発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。 |
| Expired | 現在の日付が証明書の有効期限の終了日より後です。 | 現在の日付が証明書の有効期限の終了日であるかそれより前です。 |
| Not yet valid | 現在の日付が証明書の有効期限の開始日より前です。 | 現在の日付が証明書の有効期限の開始日であるかそれより後です。 |

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| 無効な証明書 | | 証明書は有効です。以下のすべてを満たしています。<br>• 有効な証明書の拡張子。<br>• 指定した目的に証明書を使用できる。<br>• 有効な基本的制約のパス長。<br>• 有効な発行日付または有効期限の値。<br>• 有効な名前制約。<br>• 指定された目的に関してルート証明書を信頼できる。<br>• ルート証明書が指定した目的を受け入れている。 |

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| | 証明書が有効ではありません。以下の 1 つ以上を満たしています。<br>• 証明書の拡張子が無効であるか一貫していません。つまり、証明書の拡張子に無効な値（たとえば間違ったエンコーディング）が含まれているか、他の拡張子と矛盾する値がいくつか含まれています。<br>• 指定された目的に証明書を使用できません。<br>• 基本的制約のパス長パラメータを超過しています。<br>詳細については、RFC 5280、セクション 4.2.1.9 を参照してください。<br>• 証明書の発行日付または有効期限の値が無効です。これらの日付は、UTCTime または GeneralizedTime としてエンコードできます。<br>詳細については、RFC 5280、セクション 4.1.2.5 を参照してください。<br>• 名前制約の形式が認識されていません。たとえば、電子メールアドレス形式のフォームは RFC 5280、セクション 4.2.1.10 で言及されていません。これは、不適切な拡張子や、一部の新機能が現時点でサポートされていないことが原因で発生する場合があります。 | |

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| | サポートされていない名前制約タイプが見つかりました。OpenSSL では、ディレクトリ名、DNS 名、電子メール、および URI タイプのみがサポートされています。<br>• 指定された目的に関してルート認証局を信頼できません。<br>• ルート認証局が指定された目的を拒否しています。 | |
| 無効な CRL | 証明書失効リスト（CRL）のデジタル署名が有効ではありません。以下の 1 つ以上を満たしています。<br>• CRL の [次回の更新（Next Update）] または [最後の更新（Last Update）] フィールドの値が無効である。<br>• CRL がまだ有効ではない。<br>• CRL の期限が切れている。<br>• CRL パスを確認する際にエラーが発生した。拡張 CRL の確認が有効になっている場合にのみ、このエラーが発生する。<br>• CRL が検出できない。<br>• 検出できた唯一の CRL が証明書の範囲と一致しなかった。 | CRL が無効です。以下のすべてを満たしています。<br>• [次回の更新（Next Update）] と [最後の更新（Last Update）] フィールドの値が有効である。<br>• CRL の日付が有効である。<br>• パスが有効である。<br>• CRL が検出された。<br>• CRL が証明書の範囲と一致する。 |

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| サーバの不一致 | サーバ名がサーバのサーバ名指定（SNI）名と一致しません。これは、サーバ名を偽装しようとする試みを示している可能性があります。 | サーバ名は、クライアントがアクセスを要求しているサーバの SNI 名と一致します。 |

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

## 外部認証局の信頼

| スマート ライセンス | 従来のライセンス | サポートされるデバイス数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | すべて（NGIPSv を除く） | いずれか（Any） | Admin/Access Admin/Network Admin |

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようになります。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により、暗号化証明書が失効されているかどうかも確認できます。

**ステップ 1** SSL ルール エディタで、[信頼できる CA 証明書（Trusted CA Certificates）] タブを選択します。

**ステップ 2** 次のように、[使用可能な信頼できる CA（Available Trusted CAs）] で追加する信頼できる CA を見つけます。

- ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[Available Trusted CAs] リストの上にある [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 3** 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 [Select All] を選択します。

**ステップ 4** [Add to Rule] 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 5** ルールを追加するか、編集を続けます。

### 次のタスク

- TLS/SSL ルールに証明書ステータスの SSL ルール条件を追加します。詳細については、「証明書ステータスでのトラフィックの照合 （13 ページ）」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。

### 関連トピック

信頼できる認証局オブジェクト

## 信頼できる外部認証局の設定

検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。TLS/SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと照合する証明書ステータス条件を SSL ルールに設定することができます。

ヒント 信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。また、ルート発行者 CA に基づいてトラフィックを信頼するように証明書ステータス条件を設定する場合、信頼できる CA の信頼チェーン内のすべてのトラフィックは、復号する必要はなく、復号せずに許可することができます。

SSL ポリシーを作成すると、[信頼できる CA 証明書（Trusted CA Certificates）] タブにデフォルトの信頼できる CA オブジェクト グループ Cisco Trusted Authorities が入力されます。

このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。

# 証明書ステータスでのトラフィックの照合

| スマート ライセンス | 従来のライセンス | サポートされるデバイス数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | すべて（NGIPSv を除く） | いずれか（Any） | Admin/Access Admin/Network Admin |

### 始める前に

- 信頼できる CA オブジェクトまたはグループを SSL ポリシーに追加します。詳細については、外部認証局の信頼 （12 ページ）を参照してください。

**ステップ 1** Firepower Management Center で、[ポリシー（Policies）]>[アクセス コントロール（Access Control）]>[SSL] を選択します。

**ステップ 2** 新しいポリシーを追加するか、既存のポリシーを編集します。

**ステップ 3** 新しい TLS/SSL ルールを追加するか、既存のルールを編集します。

**ステップ 4** [ルールの追加（Add Rule）] または [ルールの編集（Editing Rule）] ダイアログボックスで [証明書ステータス（Cert Status）] タブを選択します。

**ステップ 5** 各証明書ステータスには次のオプションがあります。

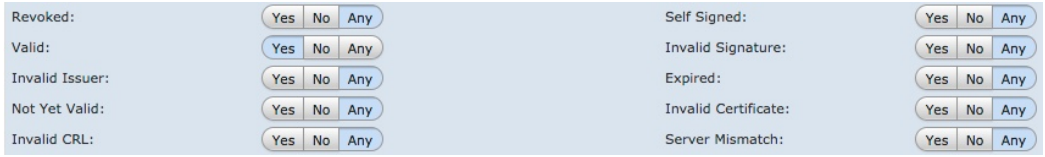
- 該当する証明書ステータスが存在するときに照合する場合は、[はい（Yes）] を選択します。
- 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ（No）] を選択します。
- ルールが一致する場合、[任意（Any）] を選択して条件をスキップします。つまり、[任意（Any）] を選択すると、証明書ステータスの有無に関わらずルールは一致します。

**ステップ 6** ルールを追加するか、編集を続けます。

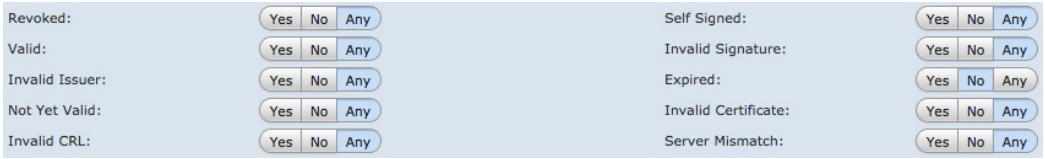
**例**

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。

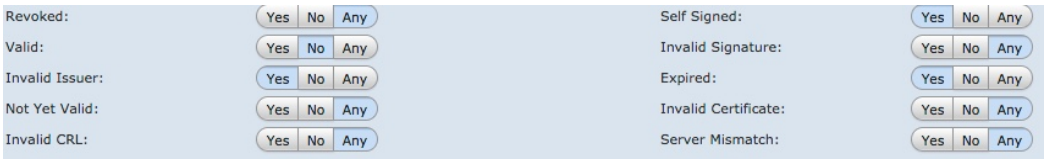
次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。



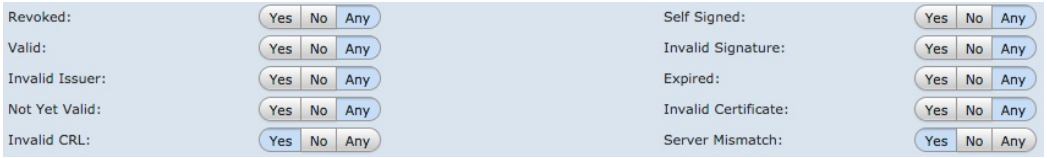

次の図は、ステータスの不在をチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックに一致し、そのトラフィックをモニタします。



次の図は、さまざまなステータスの有無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。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユーザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号します。




次の図は、要求の SNI がサーバ名に一致する、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。この設定のため、ルールがいずれかの条件に一致する場合に、トラフィックがブロックされます。




### 次のタスク

- 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。

# 暗号スイートの TLS/SSL ルール条件

暗号スイートのルール条件に追加できる、システム定義の暗号スイートが提供されています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。

（注） 新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[選択した暗号スイート（Selected Cipher Suites）] リストに最大 50 の暗号スイートおよび暗号スイートリストを追加できます。暗号スイート条件に追加できる暗号スイートとして、次のものがサポートされています。

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加すると、設定を展開できません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号がサポートされません。それらの暗号スイートを使用してルールを作成すると、アクセス コントロール ポリシーを展開できなくなります。
- 暗号スイート条件に暗号スイートを設定する場合、証明書条件に追加する外部証明書オブジェクトまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれかが、暗号スイートの署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの暗号スイート条件で EC ベースの暗号スイートを参照する場合、追加するサーバ証明書または **[復号 - 再署名（Decrypt - Resign）]** アクションに関連付ける CA 証明書も EC ベースである必要があります。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。
- SSL ルールの**暗号スイート**条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - システムは ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために TLS/SSL ルールを設定する必要があります。詳細については、SSL ルールの順序を参照してください。

- システムでは、匿名の暗号スイートで暗号化されたトラフィックは復号化できないため、ルールに **Decrypt - Resign** または **Decrypt - Known Key** アクションを使用できません。

- 暗号スイーをルール条件として指定する際、ルールをClientHelloメッセージで指定された暗号スイートの完全なリストではなく、ServerHelloメッセージのネゴシエートされた暗号スイートと照合することを検討してください。ClientHelloの処理中に、管理対象デバイスはClientHelloメッセージからサポートされていない暗号スイートを削除します。ただし、これにより指定されたすべての暗号スイートが削除されることになる場合、システムでは元のリストを保持します。システムがサポートされていない暗号スイートを保持する場合、後続の評価は復号化されないセッションになります。

# 暗号スイートによる暗号化トラフィックの制御

| スマート ライセンス | 従来のライセンス | サポートされるデバイス数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | すべて（NGIPSvを除く） | いずれか（Any） | Admin/Access Admin/Network Admin |

**ステップ 1** SSL ルール エディタで、[暗号スイート（Cipher Suite）] タブを選択します。

**ステップ 2** [使用可能な暗号スイート（Available Cipher Suites）] で、追加する暗号スイートを探します。

- ここで暗号スイートリス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）、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある追加アイコン（  ）をクリックします。
- 追加する暗号スイートおよびリストを検索するには、[Available Cipher Suites] リストの上にある [Search by name or value] プロンプトをクリックし、暗号スイートの名前または暗号スイー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、一致する暗号スイートが表示されます。

**ステップ 3** 暗号スイートをクリックして選択します。すべての暗号スイートを選択するには、右クリックして[すべて選択（Select All）] を選択します。

**ステップ 4** [ルールに追加（Add to Rule）] をクリックします。

**ヒント** 選択した暗号スイートをドラッグ 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 5** ルールを追加するか、編集を続けます。

### 次のタスク

- 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。

### 関連トピック

暗号スイート リスト

# 暗号化プロトコル バージョンの TLS/SSL ルール条件

SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、SSL バージョン 2.0 で暗号化されたトラフィックの復号化がサポートされていないためです。復号できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。

# 暗号化プロトコルのバージョンによるトラフィックの制御

| スマート ライセンス | 従来のライセンス | サポートされるデバイス数 | サポートされるドメイン数 | アクセス |
|---|---|---|---|---|
| いずれか（Any） | いずれか（Any） | すべて（NGIPSv を除く） | いずれか（Any） | Admin/Access Admin/Network Admin |

**ステップ 1** SSL ルール エディタで、[バージョン（Version）] タブを選択します。

**ステップ 2** 照合するプロトコル バージョンを選択します。

**ステップ 3** ルールを追加するか、編集を続けます。

### 次のタスク

- 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。