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

TLS/SSL のルールの条件 （2 ページ）
ユーザベースの TLS/SSL ルールの条件 （10 ページ）
暗号化トラフィックでのレピュテーションベースの URL ブロッキング （18 ページ）
サーバ証明書ベースの TLS/SSL ルール条件 （20 ページ）
ClientHello メッセージ処理

TLS/SSL のルールの条件

SSL ポリシーに追加するTLS/SSL ルールにより、暗号化トラフィックの処理やログ記録を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過する暗号化トラフィックを管理できます。以下の条件を使用できます。

- TLS/SSL ルールでゾーン条件を設定すると、暗号化トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。セキュリティ ゾーンは、複数のデバイス間に配置されている場合がある 1 つ以上のインターフェイスのグループです。
- TLS/SSL ルールでネットワーク条件を設定すると、暗号化トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御および復号できます。制御対象とする暗号化トラフィックの送信元と宛先の IP アドレスを明示的に指定するか、地理位置情報機能を使用することができます。地理位置情報機能では、IP アドレスを地理的位置に関連付けて、暗号化トラフィックをその送信元または宛先の国や大陸に基づいて制御できます。
- TLS/SSL ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。
- TLS/SSL ルールでポート条件を設定すると、暗号化トラフィックの送信元および宛先の TCP ポートに応じてそのトラフィックを制御できます。

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、TLS/SSL ルールを作成できます。これらの TLS/SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。

関連トピック

Firepower システムの IP アドレス表記法

ネットワーク ゾーン TLS/SSL ルール条件

1 つのゾーン条件で [送信元ゾーン（Sources Zones）] および [宛先ゾーン（Destination Zones）] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを離れる暗号化トラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。

  パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブなインターフェイスで構成されるゾーンを [宛先ゾーン（Destination Zones）] 条件で使用することはできません。

- 特定のゾーンのインターフェイスからデバイスに入る暗号化トラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。

送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、TLS/SSL ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とする暗号化トラフィックを照合する単一ルールを定義することはできません。

（注） インラインまたはタップ モードのインターフェイスが含まれたセキュリティ ゾーン内のトラフィックを復号化する TLS/SSL ルールの条件を作成することができますが、、トラフィックはこれらのインターフェイス上で復号化されません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ネットワーク ゾーン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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタで、[ゾーン（Zones）] タブを選択します。

ステップ 2 [利用可能なゾーン（Available Zones）] から追加するゾーンを見つけます。追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 クリックすると、ゾーンを選択できます。すべてのゾーンを選択するには、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 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ヒント 選択したゾーンをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

例

たとえば、同等に設定された追加デバイス（同じFirepower Management Centerによって管理されるもの）を展開して、複数の異なるロケーションで同様のリソースを保護できます。最初のデバイスと同様に、これらのデバイスも [内部（Internal）] セキュリティ ゾーンのアセットを保護します。

（注） 内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信する暗号化トラフィックを復号および検査してホストを保護しなければなりません。

これを実現するには、[宛先ゾーン（Destination Zone）] が [内部（Internal）] に設定されたゾーン条件を持つTLS/SSL ルールを設定します。この単純な SSL ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

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

インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

ネットワークまたは地理位置情報 TLS/SSL ルールの条件

ネットワークベースの TLS/SSL ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、再利用可能で名前を 1 つ以上の IP アドレス、アドレスブロック、

国、大陸などに関連付けるネットワーク オブジェクトおよび位置情報オブジェクトを使用してネットワーク条件を設定できます。

（注） 地理的位置別にトラフィックを制御するルールを作成して、確実に最新の位置情報データを使用してトラフィックをフィルタ処理する場合は、シスコは Firepower Management Center の位置情報データベース（GeoDB）を定期的に更新することを**強く**推奨しています。

1 つのネットワーク条件で [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに対し、最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定の IP アドレスまたは地理的位置からの暗号化トラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- 特定の IP アドレスまたは地理的位置への暗号化トラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信される暗号化トラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

関連トピック

Firepower システムの IP アドレス表記法

ネットワークまたは地理位置情報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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

始める前に

- 地理位置情報データベース（GeoDB）の更新の説明に従って、Firepower Management Center で地理位置情報データベース（GeoDB）を更新します。

手順

ステップ 1 SSL ルール エディタで、[ネットワーク（Networks）] タブを選択します。

ステップ 2 [利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけます。

- 追加するネットワーク オブジェクトとグループを表示するには[ネットワーク（Networks）] タブをクリックします。位置情報オブジェクトを表示するには [位置情報（Geolocation）] タブをクリックします。
- ネットワーク オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（  ）をクリックします。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク（Available Networks）] 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て、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。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 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 [すべて選択（Select All）] を選択します。

ステップ 4 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] 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 手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

ステップ 6 ルールを保存するか、編集を続けます。

例

次の図は、内部ネットワークから発信され、ケイマン諸島（Cayman Islands）または海外にある持ち株会社のサーバ（182.16.0.3）のリソースにアクセスしようとする暗号化接続をブロックする TLS/SSL ルールのネットワーク条件を示しています。

この例では、持ち株会社のサーバの IP アドレスを手動で指定し、ケイマン諸島の IP アドレスを表すシステム提供の地理位置情報オブジェクト Cayman Islands を使用しています。

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

ネットワーク オブジェクト
Firepower システムの IP アドレス表記法

VLAN TLS/SSL ルールの条件

VLAN ベースの TLS/SSL ルール条件を作成するときは、1 ～ 4094 の VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

ヒント VLAN タグ オブジェクトを作成しておくと、それを使用して TLS/SSL ルールを作成したり、Web インターフェイスのさまざまな場所で VLAN タグを表すオブジェクトとして使用したりできます。VLAN タグ オブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に作成することもできます。

1 つの VLAN タグ条件で、[選択済み VLAN タグ（Selected VLAN Tags）] に最大 50 の項目を追加できます。無効な VLAN タグ条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

暗号化された VLAN 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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタで、[VLAN タグ（VLAN Tags）] タブを選択します。

ステップ 2 [利用可能な VLAN タグ（Available VLAN Tags）] で、次のように追加する VLAN を見つけます。

- VLAN タグ オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ（Available VLAN Tags）] 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 VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ（Available VLAN Tags）] 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、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。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 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 [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 手動で指定する VLAN タグを追加します。[選択した VLAN タグ（Selected VLAN Tags）] リストの下にある [VLAN タグの入力（Enter a VLAN Tag）] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[追加（Add）] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

ステップ 6 ルールを保存するか、編集を続けます。

例

次の図は、特定の公開 VLAN（VLAN タグ オブジェクト グループで指定）および手動で追加した VLAN「42」上の暗号化トラフィックに一致する SSL ルールの VLAN タグ条件を示しています。

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

VLAN タグ オブジェクト

ポート TLS/SSL ルールの条件

ポートベースの TLS/SSL ルールの条件を作成するときは、手動で TCP ポートを指定できます。または、再利用可能で名前を 1 つ以上のポートに関連付けるポート オブジェクトを使用してポート条件を設定できます。

1 つのネットワーク条件で [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] それぞれに対し、最大 50 の項目を追加できます。

- 特定の TCP ポートからの暗号化トラフィックを照合するには、[選択した送信元ポート（Selected Source Ports）] を設定します。
- 特定の TCP ポートへの暗号化トラフィックを照合するには、[選択した宛先ポート（Selected Destination Ports）] を設定します。
- [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] の両方を設定すると、特定の送信元（Source）TCP ポートから発信されかつ特定の宛先（Destination）TCP ポートに送信される暗号化トラフィックが照合されます。

[選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] リストで設定できるのは TCP ポートだけです。非 TCP ポートを含むポート オブジェクトは、[使用可能ポート（Available Ports）] リストではグレイで表示されます。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、オブジェクトマネージャを使用して使用中のポート オブジェクトを編集し、それらのオブジェクト グループを使用するルールを無効にできます。アイコンの上にポインタを置くと詳細が表示されます。

ポ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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタで、[ポート（Ports）] タブを選択します。

ステップ 2 [利用可能なポート（Available Ports）] から追加する TCP ポートを次のように探します。

- TCP ポート オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能なポート（Available Ports）] 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 TCP ベースのポート オブジェクトおよびグループを検索するには、[利用可能なポート（Available Ports）] 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ポー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。たとえば、「443」と入力すると、システム提供の HTTPS ポート オブジェクトが Firepower Management Center に表示されます。

ステップ 3 TCP ベースのポート オブジェクトを 1 つ選択するには、クリックします。TCP ベースのポート オブジェクトをすべて選択するには、右クリックして [すべて選択（Select All）] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

ステップ 4 [送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] 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 送信元または宛先のポートを手動で指定するには、[選択した送信元ポート（Selected Source Ports）] または [選択した宛先ポート（Selected Destination Ports）] リストの下にある [ポート（Port）] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

ステップ 6 [追加（Add）] をクリックします。

（注） Firepower Management Centerでは、無効なポート設定はルール条件に追加されません。

ステップ 7 ルールを保存するか、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

ポート オブジェクト

ユーザベースの TLS/SSL ルールの条件

レルム、グループ、またはユーザに基づいてトラフィックと照合するように TLS/SSL ルールを設定することができます。TLS/SSL ルールのレルム、グループ、およびユーザの条件では、ユーザ制御を実行して、権威のあるユーザを IP アドレスに関連付けることにより、ネットワークを通過できるトラフィックを管理することができます。

ユーザ条件を設定した TLS/SSL ルールとトラフィックを一致させるには、モニタ対象のセッションにおける送信元または宛先ホストの IP アドレスと、ログインする権威のあるユーザを関連付ける必要があります。レルム、個々のユーザ、またはユーザが属しているグループに基づいてトラフィックを制御できます。

ユーザ ベースの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	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

始める前に

- ユーザ アイデンティティ ソースの説明に従って、1 つ以上の権限のあるユーザ アイデンティティ ソースを設定します。
- レルムの作成の説明に従って、レルムを設定します。

手順

ステップ 1 SSL ルール エディタで、[ユーザ（Users）] タブを選択します。

ステップ 2 [使用可能なレルム（Available Realms）] リストで名前または値で検索してレルムを選択します。

ステップ 3 [使用可能なユーザ（Available Users）] リストで名前または値で検索してレルムを選択します。

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 選択したユーザおよびグループをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、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。

レピュテーション ベースの TLS/SSL ルール条件

TLS/SSL ルールでレピュテーション ベース条件を設定すると、ネットワーク トラフィックをコンテキスト化して状況に応じて制限することで、ネットワーク通過を許可する暗号化トラフィックを管理できます。SSL ルールでのレピュテーション ベースの制御には、以下のタイプがあります。

- アプリケーション条件によりアプリケーション制御を実行できます。このシステムが暗号化された IP トラフィックを分析するときに、ネットワーク上で一般的に使用されている暗号化アプリケーションを識別および分類してから暗号化セッションを復号します。この

システムでは、こうした検出ベースのアプリケーション認識機能を使用して、ネットワーク上の暗号化されたアプリケーション トラフィックを制御できます。

1 つの TLS/SSL ルールにおいて、カスタム アプリケーションなどの個々のアプリケーションを選択できます。システム提供のアプリケーション フィルタを使用する。このフィルタは、基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に基づいてアプリケーションをグループ化して名前を付けたものを指します。

- URL 条件では、Web サイトに割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックを制御できます。

TLS/SSL ルールで選択したアプリケーションおよびフィルタ

シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にディテクタを更新し追加しています。独自のディテクタを作成し、そのディテクタが検出するアプリケーションに特性（リスク、関連性など）を割り当てることもできます。アプリケーション特性に基づくフィルタを使用すると、最新のディテクタを使用してアプリケーション トラフィックをモニタできます。

アプリケーション条件を設定した TLS/SSL ルールとトラフィックを一致させるには、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

（注） アクセス コントロール ルールを使用してアプリケーション トラフィックをフィルタ処理する場合、フィルタ条件としてアプリケーション タグを使用できます。ただし、暗号化トラフィックはアプリケーション タグでフィルタ処理できません。暗号化トラフィックのアプリケーションを検出するにはタグ付きの **SSL プロトコル**である必要があり、このタグが付けられていないアプリケーションは、非暗号化トラフィックまたは復号化されたトラフィックでしか検出できません。

1 つのアプリケーション条件において、最大 50 の項目を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[アプリケーション フィルタ（Application Filters）] リストからの 1 つ以上のフィルタ。この項目は、特性によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストにあるアプリケーションの検索結果を保存することで作成されたフィルタ。この項目は、部分文字列の一致によってグループ化されたアプリケーションのセットを表します。
- [Available Applications] リストからの個々のアプリケーション。

Web インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

SSL ポリシーの展開時には、一致する固有のアプリケーションのリストが、アプリケーションの条件を設定したルールごとに生成されます。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

TLS/SSL ルールのアプリケーション フィルタ

TLS/SSL ルールのアプリケーション条件を作成するには、[アプリケーション フィルタ（Application Filters）] リストを使用して、照合するトラフィックの特性を基にアプリケーションをグループ化します。

ユーザの利便性のため、各アプリケーションの特性がタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグによって判別されます。これらの基準をフィルタとして使用したり、フィルタのカスタムな組み合わせを作成してアプリケーション制御を実行したりできます。

TLS/SSL ルールにおけるアプリケーション フィルタのメカニズムは、オブジェクト マネージャを使用して再利用可能なカスタム アプリケーション フィルタを作成する場合と同じです。また、オンザフライで作成した多数のフィルタを、アクセス コントロール ルールに新規の再利用可能なフィルタとして保存できます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、カスタム フィルタはできません。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

[中（Medium）] フィルタに 110 個のアプリケーション、[高（High）] フィルタに 82 個のアプリケーションが該当する場合は、それら 192 個のアプリケーションすべてが [使用可能なアプリケーション（Available Applications）] リストに表示されます。

システムは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば Risks（リスク）タイプで Medium（中）および High（高）フィルタを選択し、Business Relevance（ビジネスとの関連性）タイプで Medium（中）および High（高）フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

この場合、システムは [中（Medium）] または [高（High）] の [リスク（Risk）] タイプと [中（Medium）] または [高（High）] の [ビジネスとの関連性（Business Relevance）] タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除します。また、Cisco 提供のフィルタ タイプ（[リスク（Risks）]、[ビジネスとの関連性（Business Relevance）]、[タイプ（Types）]、または[カテゴリ（Categories）]）を右クリックして、[すべて選択（Check All）] または [すべて選択解除（Uncheck All）] を選択することもできます。

フィルタを検索するには、[使用可能なフィルタ（Available Filters）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[使用可能なアプリケーション（Available Applications）] リストを使用して、それらのフィルタをルールに追加します。

関連トピック

アプリケーション フィルタ

ルールでTLS/SSL使用可能なアプリケーション

TLS/SSL ルールのアプリケーション条件を作成するには、[使用可能なアプリケーション（Available Applications）] リストを使用して、照合するトラフィックのアプリケーションを選択します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、システムが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン（  ）をクリックします。

一致するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション（Available Applications）] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します。フィルタを適用すると、[使用可能なアプリケーション（Available Applications）] リストが更新されます。

制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。

（注） [アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、さらに [使用可能なアプリケーション（Available Applications）] リストも検索すると、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使用して結合されます。つまり [フィルタに一致するすべてのアプリケーション（All apps matching the filter）] 条件には、[使用可能なアプリケーション（Available Applications）] リストに現在表示されている個々のすべての条件と、[使用可能なアプリケーション（Available Applications）] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。現在制約されているビューですべてのアプリケーションを選択するには、右クリックして [すべて選択（Select All）] を選択します。

1 つのアプリケーション条件において、アプリケーションの個別選択で追加できる最大数は 50 です。50 を超えるアプリケーションを追加するには、複数の TLS/SSL ルールを作成するか、フィルタを使用してアプリケーションをグループ化する必要があります。

条件のフィルタに一致するすべてのアプリケーションの選択

[アプリケーション フィルタ（Application Filters）] リストで検索またはフィルタを使用して制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。

このオプションを使用して、制約された [使用可能なアプリケーション（Available Applications）] リスト内のアプリケーションのセット全体を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに同時に追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

このようにアプリケーション条件を作成するときは、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加するフィルタの名前は、フィルタに表されているフィルタ タイプ+各タイプの最大 3 つのフィルタの名前を連結させたものとなります。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号（...）が表示されます。たとえば次のフィルタ名には、Risks（リスク）タイプの 2 つのフィルタと Business Relevance（ビジネスとの関連性）タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] で追加するフィルタに表されないフィルタ タイプは、追加するフィルタの名前に含まれません。[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リスト内のフィルタ名の上にポインタを置いたときに表示される説明テキストは、これらのフィルタ タイプが [任意（any）] に設定されていることを示します。つまり、これらのフィルタ タイプはフィルタを制約しないので、任意の値が許可されます。

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

アプリケーション ベースの TLS/SSL ルール条件の要件

アプリケーション条件を設定した TLS/SSL ルールと暗号化トラフィックを一致させるには、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

1 条件ごとに最大 50 の項目を追加でき、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。アプリケーション条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

TLS/SSL ルールへのアプリケーション条件の追加

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	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタで、[アプリケーション（Applications）] タブを選択します。

ステップ 2 [使用可能なアプリケーション（Available Applications）] リストに表示されるアプリケーションのリストをフィルタするには、[アプリケーション フィルタ（Application Filters）] リストにあるフィルタを 1 つまたは複数選択します。詳細については、TLS/SSL ルールのアプリケーション フィルタ （13 ページ）を参照してください。

ステップ 3 [使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。個々のアプリケーションを検索して選択するか、またはリストが制約されている場合は、[フィルタに一致するすべてのアプリケーション（All apps matching the

filter）] を選択できます。詳細については、ルールでTLS/SSL使用可能なアプリケーション （14 ページ）を参照してください。

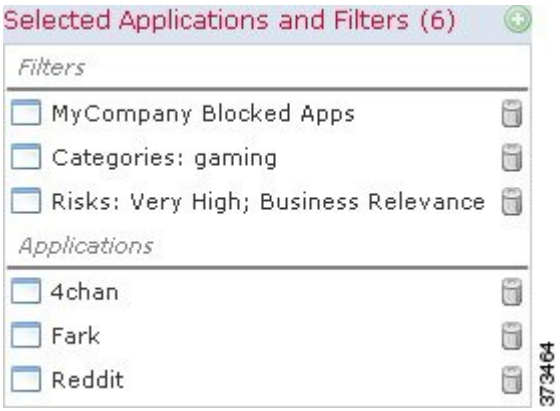
ステップ 4 [ルールに追加（Add to Rule）] をクリックします。

ヒント [すべてのフィルタをクリア（Clear All Filters）] をクリックして既存の選択をクリアします。選択したアプリケーションとフィルタをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

例

次の図は、MyCompanyのアプリケーション、リスクが高くビジネスとの関連性の低いすべてのアプリケーション、ゲーム アプリケーション、およびいくつかの指定アプリケーションからなるカスタム グループを復号化する、TLS/SSL ルールのアプリケーション条件を示しています。



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。

暗号化されたアプリケーションの制御に対する制限

暗号化されたアプリケーションの識別

このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS ClientHello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

アプリケーション識別の速度

暗号化トラフィックのアプリケーション制御は、以下のすべての処理が完了するまで実行されません。

- 暗号化された接続がクライアントとサーバ間で確立される
- 暗号化セッション内のアプリケーションがシステムにより識別される

この識別が行われるのは、サーバ証明書が交換された後です。TLS/SSL ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる TLS/SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。この問題の影響を受けるルールには、情報アイコン（）が表示されます。

システムによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに TLS/SSL ルールのアクションが適用されます。

アプリケーション ディテクタの自動有効化

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

関連トピック

ディテクタのアクティブおよび非アクティブの設定

暗号化トラフィックでのレピュテーションベースの URL ブロッキング

URL フィルタリング ライセンスでは、TLS/SSL ルールに設定した URL 条件により、要求された URL のカテゴリおよびレピュテーションに基づいて暗号化 Web サイトへのアクセスを制御できます。詳細については、URL 条件（URL フィルタリング）を参照してください。

ヒント TLS/SSL ルールで使用する URL 条件は、手動による URL フィルタリングをサポートしていません。代わりに、サブジェクト共通名を照合する識別名条件を使用してください。

URL レピュテーションに基づいた暗号化トラフィックのブロック

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	サポートされるドメイン	アクセス（Access）
URL フィルタリング	URL フィルタリング	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 SSL ルール エディタで、[カテゴリ（Category）] タブを選択します。

ステップ 2 [カテゴリ（Categories）] リストで、追加する URL カテゴリを見つけます。カテゴリを指定せずにすべての暗号化 Web トラフィックと一致させるには、[任意（Any）] カテゴリを選択します。追加可能なカテゴリを検索するには、[カテゴリ（Categories）] 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、カテゴリ名を入力します。入力すると、リストが更新されて一致するカテゴリが表示されます。

ステップ 3 カテゴリを選択するには、そのカテゴリをクリックします。

ヒント 右クリックで表示される [すべて選択（Select All）] も利用できますが、この方法ですべてのカテゴリを追加すると、TLS/SSL ルールの最大項目数 50 を超えてしまいます。代わりに [任意（Any）] を使用してください。

ステップ 4 カテゴリの選択を限定する場合は、[レピュテーション（Reputations）] リストからレピュテーション レベルをクリックする必要があります。選択できるレピュテーション レベルは 1 つだけです。レピュテーション レベルを指定しない場合、システムはデフォルトとして [任意（Any）]（つまりすべてのレベル）を設定します。

- ルールで Web アクセスのブロックまたはトラフィックの復号を行う場合（ルール アクションが、[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[復号 - 既知のキー（Decrypt - Known Key）]、[復号 - 再署名（Decrypt - Resign）]、または [モニタ（Monitor）] の場合）、選択したレピュテーション レベルよりも厳しいすべてのレピュテーションも自動的に選択されます。たとえば**疑わしいサイト（Suspicious sites）**（レベル 2）をブロックするようルールを設定した場合、**高リスク（High Risk）**（レベル 1）のサイトも自動的にブロックされます。
- ルールで Web アクセスを許可して、アクセス コントロールに従わせる場合（ルール アクションが [復号しない（Do not decrypt）] の場合）、選択したレピュテーション レベルよりも厳しくないすべてのレピュテーションも自動的に選択されます。たとえば**無害なサイト（Benign sites）**（レベル 4）を許可するようルールを設定した場合、**有名（Well known）**（レベル 5）サイトもまた自動的に許可されます。

（注） ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

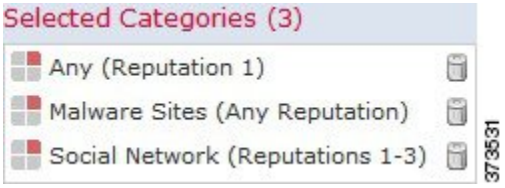
ステップ 5 [ルールに追加（Add to Rule）] をクリックして、選択した項目を [選択したカテゴリ（Selected Categories）] リストに追加します。

ヒント 選択した項目をドラッグ アンド ドロップすることもできます。

ステップ 6 ルールを保存するか、編集を続けます。

例

次の図は、すべてのマルウェア サイト、すべてのリスクの高いサイト、およびすべての安全でないソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルール例の URL 条件を示しています。



次の表では、前の図で示した条件を作成する方法を要約します。

表 *1:* 例：*URL* 条件の作成

ブロックする対象	選択するカテゴリまたは URL オブジェクト	選択するレピュテーション
マルウェア サイト（レピュテーションに関係なく）	マルウェア サイト（Malware Sites）	任意（Any）
高リスクの URL（レベル 1）	任意（Any）	1 - 高リスク（High Risk）
無害（benign）よりも大きいリスクがあるソーシャル ネットワーキング サイト（レベル 1 ～ 3）	ソーシャル ネットワーク（Social Network）	3 - セキュリティ リスクのある無害なサイト（Benign sites with security risks）

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。

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ィ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したりする場合は、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照合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を無効にしたりでき、これらのトラフィックの復号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。最初のセッションの後に、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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	すべて（NGIPSvを除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

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、[使用可能な DN（Available DNs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 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 [すべて選択（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。[サブジェクト DN（Subject DNs）] または [発行元 DN（Issuer DNs）] リストの下にある [DN または CN の入力（Enter DN or CN）] プロンプトをクリックし、共通名または識別名を入力して [追加（Add）] をクリックします。

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 [使用可能な証明書（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を照合することもでき、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、[選択した証明書（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。

- [復号 - 既知のキー（Decrypt - Known Key）] アクションも選択すると、証明書条件を設定できなくなります。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 [復号 - 再署名（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。最初のセッションの後に、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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

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、[使用可能な証明書（Available Certificates）] 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 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 [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 *2:* 証明書ステータスのルール条件の基準

ステータスの確認	[はい（Yes）] を設定	[いいえ（No）] を設定
失効（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。
自己署名（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。
有効（Valid）	以下のすべてを満たしています。 • ポリシーが証明書を発行した CA を信用できる。 • 署名は有効である。 • 発行元は有効である。 • 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。 • 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。 • 証明書を発行した CA をポリシーが信頼していない。 • 署名が無効である。 • 発行元が無効である。 • 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。 • 現在の日付が証明書の有効期間の開始日より前です。 • 現在の日付が証明書の有効期限の終了日より後です。
署名が無効（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。
発行元が無効（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。

ステータスの確認	[はい（Yes）] を設定	[いいえ（No）] を設定
期限切れ	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。
まだ無効（Not yet valid）	現在の日付が証明書の有効期間の開始日より前です。	現在の日付が証明書の有効期間の開始日であるかそれより後です。

ステータスの確認	[はい（Yes）] を設定	[いいえ（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。 • 有効な証明書の拡張子。 • 指定した目的に証明書を使用できる。 • 有効な基本的制約のパス長。 • 有効な発行日付または有効期限の値。 • 有効な名前制約。 • 指定された目的に関してルート証明書を信頼できる。 • ルート証明書が指定した目的を受け入れている。

ステータスの確認	[はい（Yes）] を設定	[いいえ（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。 • 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。 • 指定された目的に証明書を使用できません。 • 基本的制約のパス長パラメータを超過しています。 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。 • 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。 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。 • 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。	

ステータスの確認	[はい（Yes）] を設定	[いいえ（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。 • 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。 • 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。 • 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。 • CRL がまだ有効ではない。 • CRL の期限が切れている。 • 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。 • CRL が検出できない。 • 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。 • [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。 • CRL の日付が有効である。 • パスが有効である。 • CRL が検出された。 • CRL が証明書の範囲と一致する。

ステータスの確認	[はい（Yes）] を設定	[いいえ（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 証明書とその関連 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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（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。

手順

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、[使用可能な信頼できる CA（Available Trusted CAs）] 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 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 [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 （32 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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（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 （31 ページ）を参照してください。

手順

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。

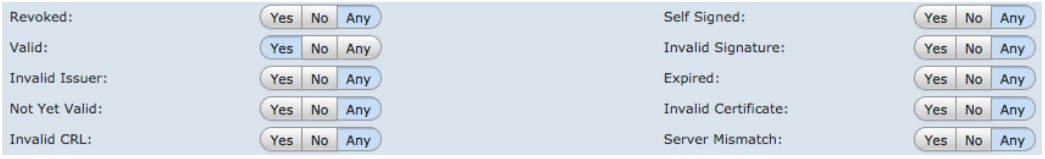
- 該当する証明書ステータスが存在するときに照合する場合は、[はい（Yes）] を選択します。
- 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ（No）] を選択します。
- ルールが一致する場合、[任意（Any）] を選択して条件をスキップします。つまり、[任意（Any）] を選択すると、証明書ステータスの有無に関わらずルールは一致します。

ステップ 6 ルールを追加するか、編集を続けます。

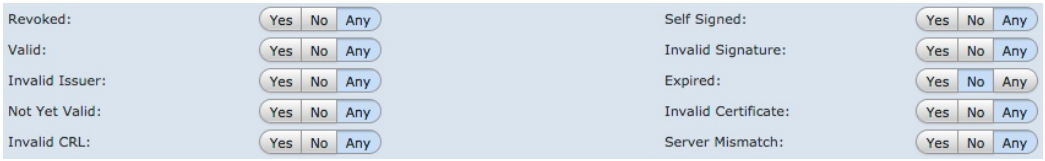
例

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。

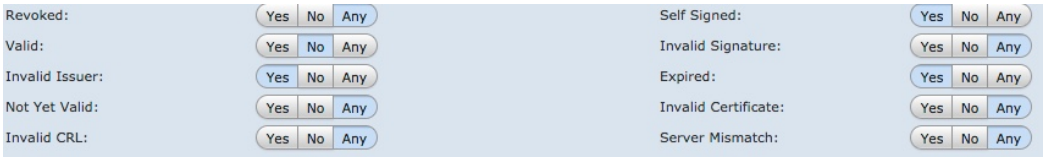
次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。



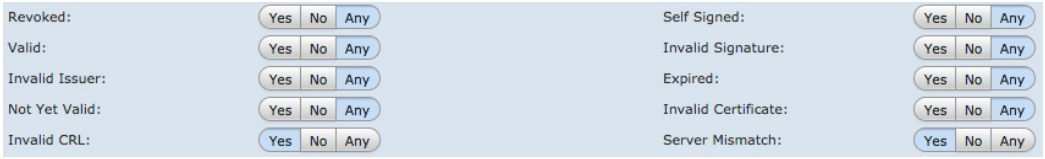
次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合し、そのトラフィックをモニタします。



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は、証明書条件に追加する外部証明書オブジェクト、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける内部 CA オブジェクトが、暗号スイートの署名アルゴリズム タイプと一致している必要があります。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。
  - ClientHello 処理中に自動的に匿名の暗号スイートが削除されます。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できないため、ルールに [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。
- 暗号スイート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、後続の評価は復号されてい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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

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、[使用可能な暗号スイート（Available Cipher Suites）] 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、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	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

手順

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。