再利用可能なオブジェクト

以下のトピックでは、Firepower システムで再利用可能オブジェクトを管理する方法について説明します。

- 再利用可能オブジェクトの概要 （2 ページ）
- オブジェクト マネージャ （4 ページ）
- ネットワーク オブジェクト （13 ページ）
- ポート オブジェクト （15 ページ）
- トンネル ゾーン （19 ページ）
- アプリケーション フィルタ （20 ページ）
- VLAN タグ オブジェクト （20 ページ）
- セキュリティ グループ タグ オブジェクト （21 ページ）
- URL オブジェクト （22 ページ）
- 地理位置情報オブジェクト （24 ページ）
- 時間範囲オブジェクト （25 ページ）
- 変数セット （26 ページ）
- セキュリティ インテリジェンスのリストとフィード （45 ページ）
- シンクホール オブジェクト （57 ページ）
- ファイル リスト （58 ページ）
- 暗号スイート リスト （64 ページ）
- 識別名オブジェクト （66 ページ）
- PKI オブジェクト （68 ページ）
- SLA モニタ オブジェクト （88 ページ）
- プレフィックス リスト （90 ページ）
- ルート マップ （92 ページ）
- アクセス リスト （96 ページ）
- AS パスのオブジェクト （100 ページ）
- コミュニティ リスト （101 ページ）
- ポリシー リスト （102 ページ）
- VPN オブジェクト （104 ページ）
- アドレス プール （120 ページ）

• FlexConfig オブジェクト （122 ページ）
• RADIUS サーバ グループ （122 ページ）

再利用可能オブジェクトの概要

柔軟性と Web インターフェイスの使いやすさを向上させるために、Firepower システムでは、名前を値に関連付ける再利用可能な構成である名前付きオブジェクトを使用します。その値を使用する場合は、代わりに名前付きオブジェクトを使用します。多くのポリシーとルール、イベント検索、レポート、ダッシュボードなど、Webインターフェイスのさまざまな場所でのオブジェクトの使用がサポートされています。よく使用される構成を表す多くの事前定義されたオブジェクトが提供されています。

オブジェクトを作成および管理するには、オブジェクトマネージャを使用します。オブジェクトを使用する多くの構成では、必要に応じて、その場でオブジェクトを作成することもできます。オブジェクト マネージャを使用して、次の操作も実行できます。

- 単一の構成で複数のオブジェクトを参照するための、オブジェクトのグループ化。オブジェクト グループ （7 ページ）を参照してください。
- 選択したデバイス、またはマルチドメイン展開の場合は選択したドメインのオブジェクト値のオーバーライド。オブジェクトのオーバーライド （9ページ）を参照してください。

アクティブなポリシーで使用されるオブジェクトを編集した後に、変更を有効にするには、変更した構成を再展開する必要があります。アクティブなポリシーで使用されているオブジェクトは削除できません。

オブジェクト タイプ

次の表に、Firepower システムで作成できるオブジェクト、各オブジェクト タイプがグループ化可能かどうか、およびオーバーライドを許可するように構成できるかどうかを示します。

オブジェクト タイプ（Object Type）	グループ化可能	オーバーライドを許可
ネットワーク	Yes	Yes
[ポート（Port）]	Yes	Yes
インターフェイス： • セキュリティ ゾーン • インターフェイス グループ	No	No
トンネル ゾーン	No	No
アプリケーション フィルタ	No	No
VLAN タグ	Yes	Yes

オブジェクト タイプ（Object Type）	グループ化可能	オーバーライドを許可
セキュリティ グループ タグ（SGT）	No	No
URL	Yes	Yes
位置情報（GeoLocation）	No	No
時間範囲	No	No
変数セット	No	No
セキュリティ インテリジェンス：ネットワーク、DNS、URL のリストとフィード	No	No
シンクホール	No	No
ファイル リスト	No	No
暗号スイート リスト	No	No
識別名（Distinguished Name）	Yes	No
公開キー インフラストラクチャ（PKI）： • 内部および信頼できる CA • 内部および外部証明書	Yes	No
SLA モニタ	No	No
プレフィックス リスト：IPv4 および IPv6	No	Yes
ルート マップ	No	Yes
アクセス リスト：標準および拡張	No	Yes
AS パス	No	Yes
コミュニティ リスト（Community List）	No	Yes
ポリシー リスト	No	Yes
FlexConfig：テキストおよびFlexConfig オブジェクト	No	Yes

オブジェクトおよびマルチテナンシー

マルチドメイン展開では、グローバルおよび子孫ドメインでオブジェクトを作成できます。ただし、グローバル ドメインでのみ作成できるセキュリティ グループ タグ（SGT）オブジェク

トを除きます。現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。また、編集できない先祖ドメインで作成されたオブジェクトも表示されますが、セキュリティ ゾーンとインターフェイス グループを除きます。

（注） セキュリティ ゾーンとインターフェイス グループは、リーフ レベルで設定したデバイス インターフェイスに関連するため、子孫ドメイン内の管理者は、先祖ドメインで作成されたゾーンとグループを表示および編集できます。サブドメインのユーザは、先祖ゾーンとグループからインターフェイスを追加および削除できますが、ゾーン/グループを削除または名前変更することはできません。

オブジェクト名は、ドメイン階層内で一意である必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

グループ化をサポートするオブジェクトの場合、現在のドメインのオブジェクトを先祖ドメインから継承されたオブジェクトとグループ化できます。

オブジェクトのオーバーライドにより、ネットワーク、ポート、VLAN タグ、URL などの特定のオブジェクト タイプのデバイス固有またはドメイン固有の値を定義できます。マルチドメイン展開では、先祖ドメイン内のオブジェクトのデフォルト値を定義できますが、子孫ドメイン内の管理者は、そのオブジェクトのオーバーライドの値を追加できます。

オブジェクト マネージャ

オブジェクト マネージャを使用すると、オブジェクトおよびオブジェクト グループを作成、管理することができます。

オブジェクト マネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーション リンクを使用して追加ページを表示します。特定のページにアクセスしたり、更新アイコン（  ）にアクセスしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。ページのオブジェクトは、名前または値でフィルタすることもできます。

オブジェクトの編集

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 リストからオブジェクト タイプを選択します（再利用可能オブジェクトの概要 （2 ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 必要に応じてオブジェクト設定を変更します。

ステップ 5 変数セットを編集する場合は、セット内の変数を管理します（変数の管理 （42 ページ）を参照）。

ステップ 6 オーバーライドを許可するように設定できるオブジェクトの場合、次の操作をします。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。現在のドメインに属しているオブジェクトに対してのみ、この設定を変更できます。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）] セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加 （11 ページ） を参照）。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 変数セットを編集するときにそのセットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

オブジェクトまたはオブジェクト グループのフィルタ処理

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの導入環境では、現在ドメインと親ドメインで作成されたオブジェクトが表示され、それらをフィルタ処理できます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [フィルタ処理（Filter）] フィールドのフィルタ条件を入力します。

ページは入力に従って更新され、一致する項目が表示されます。

次のメタ文字を使用できます。

- アスタリスク（*）文字は、ある文字の 0 回以上のオカレンスに一致します。
- キャレット記号（^）は文字列の先頭部分と一致します。
- ドル記号（$）は文字列の末尾と一致します。

オブジェクトのソート

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 列の見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

オブジェクト グループ

オブジェクトをグループ化すると、複数のオブジェクトを1つの設定で参照できます。システムでは、Web インターフェイスでオブジェクトおよびオブジェクト グループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクト グループも使用できます。

ネットワーク、ポート、VLAN タグ、URL、およびPKI オブジェクトをグループ化できます。ネットワーク オブジェクト グループはネストすることができます。つまり、ネットワーク オブジェクト グループを別のネットワーク オブジェクト グループに追加できます。許容されるネスト レベルは最大 10 です。

同じタイプのオブジェクトおよびオブジェクト グループには、同じ名前を付けることはできません。マルチドメイン展開では、オブジェクト グループの名前をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ポリシーで使用されるオブジェクト グループ（たとえば、アクセス コントロール ポリシーで使用されるネットワーク オブジェクト グループ）を編集する場合、変更を適用するためには、変更後の設定を再展開する必要があります。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、アクティブ ポリシーで使用中のグループは削除できません。たとえば、保存されたアクセス コントロール ポリシーの VLAN 条件で使用している VLAN タグのグループは削除できません。

再利用可能オブジェクトのグループ化

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

先祖ドメインから継承したオブジェクトを持つ現在のドメイン内のオブジェクトをグループ化できます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 グループ化するオブジェクトタイプが、[ネットワーク（Network）]、[ポート（Port）]、[URL]、[VLAN タグ（VLAN Tag）] の場合は、次のように操作します。

a) オブジェクト タイプのリストからオブジェクト タイプを選択します。

b) [追加 [オブジェクト タイプ]（Add [Object Type]）] ドロップダウンリストから [グループの追加（Add Group）] を選択します。

ステップ 3 グループ化するオブジェクト タイプが [識別名（Distinguished Name）] の場合は、次のように操作します。

a) [識別名（Distinguished Name）] ノードを展開します。

b) [オブジェクト グループ（Object Groups）] を選択します。

c) [識別名グループの追加（Add Distinguished Name Group）] をクリックします。

ステップ 4 グループ化するオブジェクト タイプが [PKI] の場合は、次のように操作します。

a) [PKI] ノードを展開します。

b) 次のいずれかを実行します。

- **内部 CA グループ（Internal CA Groups）**
- **信頼できる CA グループ（Trusted CA Groups）**
- **内部証明書グループ（Internal Cert Groups）**
- **外部証明書グループ（External Cert Groups）**

c) [[オブジェクト タイプ] グループの追加（Add [Object Type] Group）] ボタンをクリックします。

ステップ 5 一意の [名前（Name）] を入力します。

ステップ 6 リストから 1 つ以上のオブジェクトを選択して、[追加（Add）] をクリックします。

次のことも実行できます。

- 含める既存のオブジェクトを検索するには、フィルタ フィールド（  ）を使用します。これは入力に従って更新され、一致する項目を表示します。検索文字列をクリアするには、検索フィールドの上にある再ロード アイコン（  ）をクリックするか、検索フィールド内のクリア アイコン（）をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、すぐにオブジェクトを作成するには、追加アイコン（  ）をクリックします。

ステップ 7 必要に応じて、[ネットワーク（Network）]、[ポート（Port）]、[URL]、および [VLAN タグ（VLAN Tag）] グループに対し、次の操作を実行します。

- [説明（Description）] を入力します。

- [オーバーライドを許可する（Allow Overrides）] チェックボックスをオンにして、このオブジェクト グループのオーバーライドを許可します。オブジェクトのオーバーライドの許可 （11 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクト グループを参照する場合は、設定の変更を展開します。設定変更の導入を参照してください。

オブジェクトのオーバーライド

オブジェクトをオーバーライドすることにより、オブジェクトの代替値を定義できます。指定したデバイスに対して、システムはこの代替値を使用します。

ほとんどのデバイスに有効な定義を設定したオブジェクトを作成した後、異なる定義を必要とする少数のデバイスについて、オーバーライドを使用してオブジェクトに対する変更内容を指定できます。また、すべてのデバイスに対してオーバーライドする必要があるオブジェクトを作成し、そのオブジェクトを使用してすべてのデバイスに適用する単一のポリシーを作成することもできます。オブジェクト オーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスの必要に応じてポリシーを変更できます。

たとえば、社内のさまざまな部門への ICMP トラフィックを拒否する場合があります。それぞれの部門は、異なるネットワークに接続されています。これを実行するには、Departmental Network という名前のネットワーク オブジェクトを含むルールを使用して、アクセス コントロール ポリシーを定義します。このオブジェクトのオーバーライドを許可することによって、関連する各デバイスで、デバイスが接続されている実際のネットワークを指定するオーバーライドを作成できます。

マルチドメイン展開では、先祖ドメインのオブジェクトのデフォルト値を定義して、子孫ドメインの管理者がそのオブジェクトのオーバーライド値を追加できるようにすることができます。たとえば、マネージドセキュリティ サービス プロバイダー（MSSP）では、単一の Firepower Management Center を使用して複数の顧客のネットワーク セキュリティを管理する場合があります。この場合、MSSP の管理者は、すべての顧客の導入で使用するオブジェクトをグローバル ドメインに定義できます。各顧客の管理者は子孫ドメインにログインして、それぞれの組織に応じてそのオブジェクトをオーバーライドできます。これらのローカル管理者が MSSP の他の顧客のオーバーライド値を表示したり、影響を与えたりすることはできません。

オブジェクト オーバーライドのターゲットを特定のドメインに絞ることもできます。その場合、ユーザがデバイス レベルで値をオーバーライドしない限り、システムはターゲット ドメインのすべてのデバイスにオブジェクト オーバーライド値を使用します。

オブジェクト マネージャで、オーバーライド可能なオブジェクトを選択し、そのオブジェクトに対するデバイス レベルまたはドメイン レベルのオーバーライドのリストを定義できます。

オブジェクト オーバーライドを使用できるオブジェクト タイプは以下に限られます。

- ネットワーク
- [ポート（Port）]
- VLAN タグ
- URL
- SLA モニタ
- プレフィックス リスト
- ルート マップ
- アクセス リスト
- AS パス
- コミュニティ リスト（Community List）
- ポリシー リスト
- PKI 登録

オブジェクト マネージャでは、オーバーライド可能なオブジェクトのオブジェクト タイプには [オーバーライド（Override）] 列が表示されます。この列の有効な値は以下のとおりです。

- 緑のチェックマーク：このオブジェクトにはオーバーライドを作成できます。オーバーライドはまだ追加されていません。
- 赤の X：このオブジェクトにはオーバーライドを作成できません。
- 数値：このオブジェクトに追加されているオーバーライドの数を表します（たとえば、「2」は 2 つのオーバーライドが追加されていることを意味します）。

オブジェクト オーバーライドの管理

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから選択します（再利用可能オブジェクトの概要 （2 ページ）を参照）。

ステップ 3 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、上書きを許可しないように設定されており、オブジェクトを変更する権限がありません。

ステップ 4 オブジェクト オーバーライドを管理します。

- 追加：オブジェクト オーバーライドを追加します（オブジェクトのオーバーライドの追加（11 ページ）を参照）。
- 許可：オブジェクト オーバーライドを許可します（オブジェクトのオーバーライドの許可（11 ページ）を参照）。
- 削除：オブジェクト エディタで、削除するオーバーライドの横にある削除アイコン（  ）をクリックします。
- 編集：オブジェクト オーバーライドを編集します（オブジェクト オーバーライドの編集（12 ページ）を参照）。

オブジェクトのオーバーライドの許可

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 オブジェクト エディタで、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします。

ステップ 2 [保存（Save）] をクリックします。

次のタスク

- オブジェクトのオーバーライド値を追加します（オブジェクトのオーバーライドの追加（11 ページ）を参照）。

オブジェクトのオーバーライドの追加

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）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

始める前に

- オブジェクトのオーバーライドを許可します（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

手順

ステップ 1 オブジェクト エディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ターゲット（Targets）] タブで、[使用可能なデバイスとドメイン（Available Devices and Domains）] リストからドメインまたはデバイスを選択し、[追加（Add）] をクリックします。

ステップ 4 [オーバーライド（Override）] タブで、[名前（Name）] を入力します。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 オーバーライド値を入力します。

例：

ネットワーク オブジェクトについては、ネットワーク値を入力します。

ステップ 7 [追加（Add）] 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

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

オブジェクト オーバーライドの編集

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

既存のオーバーライドの説明と値を変更できます。ただし、既存のターゲット リストは変更できません。代わりに、既存のオーバーライドを置き換える、新しいターゲットに対する新しいオーバーライドを追加する必要があります。

手順

ステップ 1 オブジェクト エディタで、[オーバーライド（Override）] セクションを展開します。

ステップ 2 変更するオーバーライドの横にある編集アイコン（  ）をクリックします。

ステップ 3 必要に応じて、[説明（Description）] を変更します。

ステップ 4 オーバーライド値を変更します。

ステップ 5 [保存（Save）] をクリックして、オーバーライドを保存します。

ステップ 6 [保存（Save）] をクリックして、オブジェクトを保存します。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

ネットワーク オブジェクト

ネットワーク オブジェクトは 1 つ以上の IP アドレスを表します。ネットワーク オブジェクトおよびグループを、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、アイデンティティ ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で使用できます。

ネットワーク オブジェクトを必要とするオプションを設定する際は、リストが自動的にフィルタリングされて、そのオプションに有効なネットワーク オブジェクトだけが表示されます。たとえば、オプションのなかにはホスト オブジェクトが必要なものと、サブネットが必要なものがあります。

ネットワーク オブジェクトには、以下のいずれかのタイプを指定できます。

ホスト

単一の IP アドレス。

IPv4 の例：

```
209.165.200.225
```

IPv6 の例：

`2001:DB8::0DB8:800:200C:417A` または `2001:DB8:0:0:0DB8:800:200C:417A`

ネットワーク（Network）

アドレス ブロック（別名サブネット）。

IPv4 の例：

```
209.165.200.224/27
```

IPv6 の例：

```
2001:DB8:0:CD30::/60
```

アドレス範囲（Address Range）

IP アドレスの範囲。

IPv4 の例：

```
209.165.200.225-209.165.200.250
```

IPv6 の例：

```
2001:db8:0:cd30::1-2001:db8:0:cd30::1000
```

グループ

ネットワーク オブジェクトまたは他のネットワーク グループからなるグループ。

次に例を示します。

```
209.165.200.225
209.165.201.1
209.165.202.129
```

あるネットワーク オブジェクト グループを別のネットワーク オブジェクト グループに追加することで、ネストされたグループを作成できます。グループをネストできるレベルは、最大で 10 レベルです。

ネットワーク オブジェクトの作成

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ネットワーク（Network）] を選択します。

ステップ 3 [ネットワークを追加（Add Network）] ドロップダウン メニューで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 [ネットワーク（Network）] フィールドに、適切な値を入力します。ネットワーク オブジェクト （13 ページ）を参照してください。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）] セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加 （11 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

ポート オブジェクト

ポート オブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

TCP および UDP

ポート オブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例：`TCP(6)/22`。

ICMP および ICMPv6（IPv6-ICMP）

ポート オブジェクトはインターネット層プロトコルと、オプションでタイプおよびコードを表します。例：`ICMP(1):3:3`

ICMP または IPV6-ICMP ポート オブジェクトは、タイプ、および該当する場合はコードを基準に制限できます。ICMP のタイプとコードの詳細については、次の URL を参照してください。

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

その他

ポート オブジェクトは、ポートを使用しない他のプロトコルを表します。

Firepower システムには、ウェルノウン ポート用にデフォルトのポート オブジェクトが用意されています。これらのデフォルト オブジェクトを変更または削除することはできません。デフォルト オブジェクトに加え、カスタム ポート オブジェクトを作成できます。

ポート オブジェクトおよびグループは、アクセス コントロール ポリシー、アイデンティティ ルール、ネットワーク検出ルール、ポート変数、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、組織が特定のポート範囲を使用するカ

スタムクライアントを使用していて、システムで過剰なイベントや誤解を与えるイベントが発生した場合、それらのポートをモニタ対象から除外するようネットワーク検出ポリシーを設定できます。

ポート オブジェクトを使用する際は、次のガイドラインに従ってください。

- アクセス コントロール ルールの送信元ポート条件にはTCP/UDP以外のプロトコルを追加できません。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポート プロトコルを混在させることはできません。
- 送信元ポート条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、設定を展開しても、その条件が使用されているルールは管理対象デバイスで適用されません。
- TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポート条件としてそのポートオブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

ポート オブジェクトの作成

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ポート（Port）] を選択します。

ステップ 3 [ポートの追加（Add Port）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

ステップ 5 [プロトコル（Protocol）] を選択します。

ステップ 6 選択したプロトコルに応じて、[ポート（Port）] で制限するか、またはICMPの[タイプ（Type）] および [コード（Code）] を選択します。

1 から **65535** のポートを入力できます。ポート範囲を指定するには、ハイフンを使用します。[すべて（All）] のプロトコルと一致させることを選択した場合は、[その他（Other）] ドロップダウン リストを使用して、ポートでオブジェクトを制限する必要があります。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）] セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加 （11 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

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

インターフェイス オブジェクトは、ネットワークをセグメント化してトラフィック フローを制御し、分類しやすくします。インターフェイス オブジェクトは単にインターフェイスをグループ化します。これらのグループは複数のデバイスにまたがることがあります。また、単一のデバイスに複数のインターフェイス オブジェクトを設定することもできます。

インターフェイス オブジェクトには次の 2 つのタイプがあります。

- セキュリティ ゾーン：インターフェイスは、1 つのセキュリティ ゾーンにのみ属することができます。
- インターフェイス グループ：インターフェイスは複数のインターフェイスグループ（および 1 つのセキュリティ ゾーン）に属することができます。

  Firepower Threat Defense NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーでインターフェイスグループを使用できます。

トンネルゾーンはインターフェイスオブジェクトではありませんが、特定の設定ではセキュリティ ゾーンの代わりにトンネルゾーンを使用できます。トンネル ゾーンおよびプレフィルタリングを参照してください。

インターフェイスオブジェクト内のすべてのインターフェイスが同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があります。インターフェイスオブジェクトを作成した後、それに含まれるインターフェイスのタイプを変更することはできません。

オブジェクト マネージャのインターフェイス オブジェクトのページでは、管理対象デバイスで設定されているセキュリティ ゾーンとインターフェイス グループの一覧が表示されます。また、このページには、各インターフェイス オブジェクトのタイプも表示され、各インター

フェイスオブジェクトを展開すると、どのデバイスのどのインターフェイスが各オブジェクトに属するかを表示できます。

モデル固有の注意事項および警告

7000 または 8000 シリーズ デバイスの初期設定時に、システムはデバイス用に選択した検出モードに基づいてセキュリティゾーンを作成します。たとえば、パッシブ展開ではシステムはパッシブゾーンを作成し、インライン展開では外部ゾーンと内部ゾーンを作成します。Firepower Management Center にデバイスを登録すると、これらのセキュリティゾーンが Management Center に追加されます。

ASA FirePOWER セキュリティ コンテキストの変更（シングル コンテキスト モードからマルチコンテキストモードへの変更、またはその逆の変更）をすると、割り当てられているセキュリティ ゾーンからデバイスのすべてのインターフェイスがシステムによって削除されます。

インターフェイス オブジェクトとマルチテナンシー

マルチドメイン展開では、どのレベルでもインターフェイス オブジェクトを作成できます。先祖ドメインで作成されたインターフェイス オブジェクトには別のドメインのデバイスに存在するインターフェイスが含まれる場合があります。この状況において、オブジェクト マネージャ内の先祖のインターフェイス オブジェクトの設定を表示するサブドメイン ユーザには、当該ドメインのインターフェイスのみが確認できます。

ロールによって制限されない限り、サブドメインのユーザは先祖ドメインで作成されたインターフェイス オブジェクトを表示**および**編集できます。サブドメインのユーザは、これらのインターフェイス オブジェクトにインターフェイスの追加や削除を行えます。ただし、インターフェイス オブジェクトの削除や名称変更はできません。子孫ドメインで作成されたインターフェイス オブジェクトの表示や編集はできません。

セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成

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）	セキュリティ ゾーン：任意 インターフェイス グループ：Firepower Threat Defense	任意（Any）	Admin/Access Admin/Network Admin

ヒント 空のインターフェイス オブジェクトを作成し、後からインターフェイスを追加できます。インターフェイスを追加するには、インターフェイスに名前が付いている必要があります。**[デバイス（Devices）]>[デバイス管理（Device Management）]** でインターフェイスを設定しているときに、セキュリティ ゾーンを作成することもできます（インターフェイス グループは作成できません）。

始める前に

- 各種インターフェイス オブジェクトの使用要件および制限を理解します。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 （17 ページ）を参照してください。
- 必要なインターフェイス オブジェクトを慎重に決定します。既存のセキュリティ ゾーンをインターフェイス グループに、またはその逆に変更することはできません。代わりに、新しいインターフェイス オブジェクトを作成する必要があります。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから、**[インターフェイス（Interface）]** を選択します。

ステップ 3 **[追加（Add）] > [セキュリティ ゾーン（Security Zone）]** または **[追加（Add）] > [インターフェイス グループ（Interface Group）]** をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [インターフェイス タイプ（Interface Type）] を選択します。

ステップ 6 **[デバイス（Device）] > [インターフェイス（Interfaces）]** ドロップダウン リストから、追加するインターフェイスを含むデバイスを選択します。

ステップ 7 1 つ以上のインターフェイスを選択します。

ステップ 8 [追加（Add）] をクリックして、デバイス別にグループ化された、選択したインターフェイスを追加します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

トンネル ゾーン

トンネル ゾーンとは、特別な分析のために明示的にタグ付けする特定のタイプのプレーン テキスト、パススルー トンネルを表します。トンネル ゾーンは、一部の設定でインターフェイスの制約として使用できますが、インターフェイス オブジェクトではありません。

詳細については、トンネル ゾーンおよびプレフィルタリングを参照してください。

アプリケーション フィルタ

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。オブジェクト マネージャで、システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザ定義の再利用可能アプリケーション フィルタを作成、管理できます。詳細については、アプリケーション条件（アプリケーション制御）を参照してください。

VLAN タグ オブジェクト

設定した個々のVLANタグ オブジェクトは、1つのVLANタグまたはタグの範囲を表します。

複数の VLAN タグ オブジェクトをグループ化できます。グループは複数のオブジェクトを表します。つまり、1つのオブジェクトでVLANタグの範囲を使用することは、この意味ではグループとはみなされません。

VLANタグ オブジェクトとグループは、ルールやイベント検索など、システムのWebインターフェイスのさまざまな場所で使用できます。たとえば、特定の VLAN だけに適用されるアクセス コントロール ルールを作成することができます。

VLAN タグ オブジェクトの作成

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）	任意（Any）	任意（Any）	Admin Access Admin Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

ステップ 2 オブジェクト タイプのリストから [VLAN タグ（VLAN Tag）] を選択します。

ステップ 3 [VLAN タグの追加（Add VLAN Tag）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 [名前（Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 [VLANタグ（VLAN Tag）]フィールドに値を入力します。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 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）] セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加 （11 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

セキュリティ グループ タグ オブジェクト

セキュリティ グループ タグ（SGT）オブジェクトは、単一の SGT 値を指定します。ルールで SGT オブジェクトを使用して、Cisco ISE で割り当てられたものでは**ない** SGT 属性を持つトラフィックを制御できます。SGT オブジェクトをグループ化またはオーバーライドすることはできません。

関連トピック

カスタム セキュリティ グループ タグ（SGT）から ISE セキュリティ グループ タグ（SGT）への自動遷移

カスタム SGT 条件

ISE SGT とカスタム SGT ルール条件との比較

セキュリティ グループ タグ オブジェクトの作成

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	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- ISE/ISE-PIC 接続を無効にします。アイデンティティ ソースとして ISE/ISE-PIC を使用している場合は、カスタム SGT オブジェクトを作成することはできません。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [セキュリティ グループ タグ（Security Group Tag）] を選択します。

ステップ 3 [セキュリティ グループ タグの追加（Add Security Group Tag）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 [タグ（Tag）] フィールドに、単一の SGT を入力します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

関連トピック

カスタム セキュリティ グループ タグ（SGT）から ISE セキュリティ グループ タグ（SGT）への自動遷移
カスタム SGT 条件
ISE SGT とカスタム SGT ルール条件との比較

URL オブジェクト

設定した各 URL オブジェクトは、単一の URL または IP アドレスを表します。URL オブジェクトとグループは、アクセス コントロール ポリシーやイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の Web サイトをブロックするアクセス コントロール ルールを作成することができます。

URL オブジェクトを作成する際に、特に暗号化トラフィックを復号またはブロックする SSL インスペクションを設定しない場合は、次の事項に留意してください。

- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル（HTTP 対 HTTPS）を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィックがブロックされます。URL オブジェク

トを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com/` ではなく、`example.com` を使用します。

URL オブジェクトの作成

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [URL] を選択します。

ステップ 3 [URL の追加（Add URL）] ドロップダウン リストで、[オブジェクトの追加（Add Object）] を選択します。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 [URL] に、URL または IP アドレスを入力します。

ステップ 7 オブジェクトのオーバーライドを管理します。

- このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。
- このオブジェクトにオーバーライド値を追加する場合は、[オーバーライド（Override）] セクションを展開し、[追加（Add）] をクリックします（オブジェクトのオーバーライドの追加 （11 ページ） を参照）。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

地理位置情報オブジェクト

設定済みの位置情報（ジオロケーション）オブジェクトは、モニタ対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。アクセス コントロール ポリシー、SSL ポリシー、イベント検索など、システムの Web インターフェイスのさまざまな場所で地理位置情報オブジェクトを使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセス コントロール ルールを作成できます。

常に最新の情報を使用してネットワーク トラフィックをフィルタ処理できるように、地理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お勧めします。

地理位置情報オブジェクトの作成

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [地理位置情報（Geolocation）] を選択します。

ステップ 3 [位置情報の追加（Add Geolocation）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 地理位置情報オブジェクトに含める国および大陸のチェック ボックスを選択します。大陸を選択すると、その大陸内のすべての国、および GeoDB 更新によってその大陸に今後追加されるすべての国が選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

時間範囲オブジェクト

指定した時間にのみポリシーを適用するには、時間範囲オブジェクトを使用します。

時間範囲オブジェクトの作成

指定した時間範囲の間にのみポリシーを適用する場合は、時間範囲オブジェクトを作成してから、そのオブジェクトをポリシーで指定します。

時間範囲オブジェクトは、VPN グループ ポリシー オブジェクトでのみ指定できます。

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2 オブジェクト タイプのリストから [時間範囲（Time Range）] を選択します。

ステップ 3 [時間範囲の追加（Add Time Range）] をクリックします。

ステップ 4 値を入力します。

次のガイドラインに従ってください。

- 入力したオブジェクト名の周りに赤色のエラー ボックスが表示された場合は、[名前（Name）] フィールドの上にマウスを置くと名前付けの制限が表示されます。
- 時間はすべて UTC です。
- 24 時間制で時間を入力します。たとえば、1:30 PM は 13:30 と入力します。
- 通常の週末の時間（夕方および夜を含む、金曜日の 5pm から月曜日の 8am まで）など、1 つの連続する範囲を指定するには、[範囲タイプ（Range Type）] に [範囲（Range）] を選択します。
- 月曜日から金曜日の 8am から 5pm まで（各日の夕方、夜、早朝を除く）など、複数の日の一部分を指定する場合は、[範囲タイプ（Range Type）] に [日次間隔（Daily Interval）] を選択します。
- 同じ曜日の複数の非連続時間、または異なる曜日の異なる時間を指定する場合は、繰り返し間隔を複数作成します。たとえば、標準の営業時間を除くすべての時間にポリシーを適用する場合は、次の 2 つの繰り返し間隔を持つ 1 つの時間範囲オブジェクトを作成します。
  - 月曜日から金曜日の 5pm から 8am の [日次間隔（Daily Interval）]、および
  - 金曜日の 5pm から月曜日の 8am までの [範囲（Range）] の繰り返し間隔。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

[アクセス時間（Access Hours）] フィールドを使用して、VPN グループ ポリシー オブジェクトに時間範囲オブジェクトを指定します。

詳細については、グループ ポリシー オブジェクトの設定 （112 ページ） および グループ ポリシーの詳細オプション （117 ページ） を参照してください。

変数セット

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーで変数を使用して、ルール抑制、アダプティブ プロファイルの更新、および動的（ダイナミック）ルール状態で IP アドレスを表すこともできます。

ヒント プリプロセッサ ルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。システム提供のデフォルトの変数セットを使用することも、独自のカスタムセットを作成することもできます。いずれのセット内でも、定義済みのデフォルト変数を変更したり、ユーザ定義変数を追加および変更したりできます。

Firepower システムで提供する共有オブジェクト ルールと標準テキスト ルールのほとんどで、定義済みのデフォルト変数を使用してネットワークとポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ルールがより効率的なのは、変数がユーザのネットワーク環境をより正確に反映する場合です。少なくとも、デフォルトセットにあるデフォルト変数は変更する必要があります。`$HOME_NET` などの変数がネットワークを正しく定義し、`$HTTP_SERVERS` にネットワーク上のすべての Web サーバが含まれていれば、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムがモニタされます。

変数を使用するには、変数セットをアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセス コントロール ポリシーによって使用されるすべての侵入ポリシーにリンクされています。

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。どの変数セット内でも、ユーザ定義変数を追加し、任意の変数の値をカスタマイズすることができます。

Firepower システムでは、初めに定義済みのデフォルト値で構成された単一のデフォルトの変数セットを提供します。デフォルトセット内の各変数は、最初はそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値は Cisco Talos Security Intelligence and Research Group（Talos）によって設定され、ルール更新で提供される値です。

定義済みのデフォルト変数は、そのデフォルト値に設定されたままにすることもできますが、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルトセットでのみ使用できますが、多くの場合、1 つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の現在値によって、他のすべてのセットの変数のデフォルト値が決まることに注意してください。

[オブジェクト マネージャ（Object Manager）] ページで [変数セット（Variable Sets）] を選択した場合、オブジェクトマネージャには、デフォルトの変数セットと、作成したすべてのカスタム セットがリストされます。

新しくインストールされたシステムでは、デフォルトの変数セットは、Cisco で定義済みのデフォルト変数だけで構成されています。

各変数セットには、システムによって提供されるデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルトセットの名前を変更したり、削除したりすることはできないことに注意してください。

マルチドメイン展開では、システムはサブドメインごとにデフォルトの変数セットを生成します。

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

関連トピック

変数の管理 （42 ページ）
変数セットの管理 （40 ページ）

侵入ポリシー内の変数セット

Firepower システムは、デフォルトではアクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルトの変数セットをリンクします。侵入ポリシーを使用するアクセス コントロール ポリシーを展開すると、その侵入ポリシー内で有効にした侵入ルールでは、リンクされた変数セットの変数値が使用されます。

アクセス コントロール ポリシー内の侵入ポリシーで使用されるカスタム変数セットを変更すると、システムの [アクセス コントロール ポリシー（Access Control Policy）] ページで、そのポリシーのステータスが「失効（out-of-date）」と表示されます。変数セットの変更内容を実

装するには、アクセス コントロール ポリシーを再度展開する必要があります。デフォルトセットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効（out-of-date）」と表示され、変更内容を実装するにはすべてのアクセス コントロール ポリシーを再度展開する必要があります。

変数

変数は、次のカテゴリのいずれかに属します。

デフォルト変数

Firepower システムから提供される変数。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。ただし、デフォルト変数のカスタマイズしたバージョンを作成できます。

カスタマイズされた変数

作成した変数。この変数には、次の変数があります。

- カスタマイズされたデフォルト変数

  デフォルト変数の値を編集すると、システムはその変数を[デフォルトの変数（Default Variables）] 領域から [カスタマイズされた変数（Customized Variables）] 領域に移動します。デフォルト セットの変数値によってカスタム セットの変数のデフォルト値が決まるため、デフォルトセットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

- ユーザ定義変数

  独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットすると、それは[カスタマイズされた変数（Customized Variables）] 領域に残ります。

  ユーザ定義変数は、次のいずれかのタイプにできます。

  - ネットワーク変数は、ネットワーク トラフィックのホストの IP アドレスを指定します。
  - ポート 変数は、ネットワーク トラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 `any` を指定することもできます。

たとえば、カスタム標準テキストルールを作成する場合、独自のユーザ定義変数を追加して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化したりすることもできます。また、「緩衝地帯」（つまり DMZ）でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリストされる `$DMZ` という変数を作成することもできます。こうして、この地帯で作成された任意のルールで `$DMZ` 変数を使用できます。

拡張変数

特定の条件下で Firepower システムから提供される変数。この変数が含まれる展開は非常に限定的です。

定義済みデフォルト変数

デフォルトでは、Firepower System は、1 つのデフォルト変数セットを提供します。このセットは、定義済みのデフォルト変数から構成されています。Cisco Talos Security Intelligence and Research Group（Talos） では、ルール更新を使用し、新しい侵入ルールや更新された侵入ルール、他の侵入ポリシー エレメント（デフォルト変数など）を提供します。

システムが提供する侵入ルールの多くが定義済みのデフォルト変数を使用していることから、これらの変数に関する適切な値を設定します。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更できます。

⚠

注意 アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。

次の表では、システムによって提供される変数について説明し、通常、いずれの変数が変更されるかを示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートに問い合わせてください。

表 *1*: システム提供変数

変数名	説明	変更しますか
$AIM_SERVERS	既知の AOL インスタント メッセンジャ（AIM）サーバを定義し、これらはチャット ベースのルールや AIM エクスプロイトを検索するルールで使用されます。	不要。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバに特に影響するルールを作成する場合、$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルール セットでは不要です。
$EXTERNAL_NET	Firepower System が非保護ネットワークとして表示されるネットワークを定義し、外部ネットワークを定義する多くのルールで使用されます。	はい。$HOME_NET を適切に定義してから、$EXTERNAL_NET の値として $HOME_NET を除外する必要があります。

変数名	説明	変更しますか
$FILE_DATA_PORTS	ネットワーク ストリームでファイルを検出する侵入ルールで使用される非暗号化ポートを定義します。	不要。
$FTP_PORTS	ネットワーク上のFTPサーバのポートを定義し、FTPサーバのエクスプロイト ルールに使用されます。	はい。FTPサーバがデフォルト ポート以外のポートを使用する場合（webインターフェイスのデフォルト ポートを表示できます）。
$GTP_PORTS	パケット デコーダがGTP（General Packet Radio Service（GPRS）トンネリング プロトコル）PDU内部でペイロードを取得するデータ チャネル ポートを定義します。	不要。
$HOME_NET	関連した侵入ポリシーがモニタするネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークのIPアドレスを指定する場合は変更します。
$HTTP_PORTS	ネットワーク上のWebサーバのポートを定義し、Webサーバのエクスプロイト ルールに使用されます。	はい。webサーバがデフォルト ポート以外のポートを使用する場合（webインターフェイスのデフォルト ポートを表示できます）。
$HTTP_SERVERS	ネットワーク上のWebサーバを定義します。Webサーバのエクスプロイト ルールで使用されます。	HTTPサーバを実行する場合は変更します。
$ORACLE_PORTS	ネットワーク上でOracleデータベース サーバのポートを定義し、Oracleデータベースでの攻撃をスキャンするルールで使用されます。	Oracleサーバを実行する場合は変更します。
$SHELLCODE_PORTS	システムにシェルコードのエクスプロイトをスキャンさせるポートを定義し、シェルコードを使用するエクスプロイトを検出するルールで使用されます。	不要。
$SIP_PORTS	ネットワーク上のSIPサーバのポートを定義し、SIPのエクスプロイト ルールに使用されます。	不要。

変数名	説明	変更しますか
$SIP_SERVERS	ネットワーク上の SIP サーバを定義し、SIP 対象エクスプロイトを指定するルールで使用されます。	はい。SIP サーバを実行している場合は、$HOME_NET を適切に定義してから、$SIP_SERVERS の値として $HOME_NET を含める必要があります。
$SMTP_SERVERS	ネットワーク上で SMTP サーバを定義し、メールサーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTP サーバを実行する場合は変更します。
$SNMP_SERVERS	ネットワーク上で SNMP サーバを定義し、SNMP サーバでの攻撃をスキャンするルールで使用されます。	SNMP サーバを実行する場合は変更します。
$SNORT_BPF	その後バージョン 5.3.0 以降にアップグレードされるバージョン 5.3.0 以前の Firepower System ソフトウェア リリースのシステム上に存在する場合のみに表示されるレガシー拡張変数を特定します。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
$SQL_SERVERS	ネットワーク上のデータベース サーバを定義し、データベース対象エクスプロイトを指定するルールで使用されます。	はい。SQL サーバを実行する場合は変更します。
$SSH_PORTS	ネットワーク上の SSH サーバのポートを定義し、SSH サーバのエクスプロイト ルールに使用されます。	はい。デフォルト ポート以外の SSH サーバのポートを使用する場合（web インターフェイスでのデフォルト ポートを表示できます）。
$SSH_SERVERS	ネットワーク上の SSH サーバを定義し、SSH 対象エクスプロイトを指定するルールで使用されます。	はい。SSH サーバを実行している場合は、$HOME_NET を適切に定義してから、$SSH_SERVERS の値として $HOME_NET を含める必要があります。
$TELNET_SERVERS	ネットワーク上の既知の Telnet サーバを定義し、Telnet サーバ対象エクスプロイトを指定するルールで使用されます。	Telnet サーバを実行する場合は変更します。

変数名	説明	変更しますか
$USER_CONF	Webインターフェイスを介して利用可能できる場合を除き、1 つ以上の特徴を設定できる一般的なツールを提供します。 $USER_CONF の設定が競合または重複していると、システムは停止します。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

ネットワーク変数

ネットワーク変数で表される IP アドレスを、侵入ポリシーで有効にした侵入ルール、侵入ポリシー ルール抑制、動的ルール状態、およびアダプティブ プロファイルの更新で使用することができます。ネットワーク変数とネットワーク オブジェクトおよびネットワーク オブジェクト グループとの相違点として、ネットワーク変数は侵入ポリシーおよび侵入ルールに固有のものです。一方、ネットワーク オブジェクトおよびグループを使用すると、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイスのさまざまな場所で IP アドレスを表すことができます。

次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール：侵入ルールの [送信元 IP（Source IPs）] および [宛先 IP（Destination IPs）] 見出しフィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。
- 抑制：送信元または宛先の侵入ルール抑制の [ネットワーク（Network）] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。
- 動的ルール状態：送信元または宛先の動的ルール状態の [ネットワーク（Network）] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサ ルールの一致数が多すぎる場合に、それを検出できます。
- アダプティブ プロファイルの更新：アダプティブ プロファイルの更新が有効にされている場合、アダプティブ プロファイルの [ネットワーク（Networks）] フィールドに、パッシブ展開でパケット フラグメントおよび TCP ストリームのリアセンブルを改善する必要があるホストが示されます。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセス コントロール ポリシーで処理されるネットワーク トラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ

- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のネットワーク オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）
- リテラルの単一 IP アドレスまたはアドレス ブロック

  それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は `any` で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は `none` です。これは「ネットワークなし」を意味します。また、リテラル値の中でアドレス `::` を指定すると、包含ネットワーク リストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレス ブロックが除外されます。つまり、除外された IP アドレスやアドレス ブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラル アドレス `192.168.1.1` を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、`2001:db8:ca2e::fa4c` を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラル ネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 `192.168.1.1` および `192.168.1.5` を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが含まれます。つまり、システムはこの構文を「192.168.1.1 **でなく、しかも** 192.168.1.5 **でない**」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワーク リストに、値 `any` を持つ変数を追加することはできません。
- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレス ブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。

ポート変数

ポート変数は、侵入ポリシーで有効になった侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP や UDP 以外のプロトコル

用にポート オブジェクトを作成して、ポート変数、アクセス コントロール ポリシー、ネットワーク検出ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。

侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] ヘッダー フィールドでポート変数を使用すると、パケット インスペクションを特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、アクセス コントロール ポリシーが展開されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

  使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。

- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のポート オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

  有効な変数値は TCP および UDP ポートのみです（どちらのタイプでも値 `any` を含む）。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効なポート オブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクト リストには表示されません。オブジェクト マネージャを使用して、変数で使われるポート オブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラル ポート値とポート範囲

  ポート範囲はダッシュ（-）を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

  複数のリテラル ポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わせることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は `any` で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は `none` で、これは「ポートなし」を示します。

ヒント 値 `any` を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

- 論理的に言って、値 any を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 any を持つ変数を除外ポートリストに追加した場合、変数セットを保存することはできません。
- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が除外されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。

拡張変数

拡張変数を使用すると、他の方法では Web インターフェイスで設定できない機能を設定することができます。現在、Firepower システムで使用可能な拡張変数は 2 つのみで、そのうち USER_CONF 拡張変数のみ編集可能です。

USER_CONF

USER_CONF は、Web インターフェイスで通常設定できない 1 つ以上の機能を設定するための汎用ツールです。

⚠

注意 機能の説明またはサポート担当の指示に従う場合を除き、拡張変数USER_CONFを使用して侵入ポリシー機能を設定**しないで**ください。競合または重複する設定が存在すると、システムが停止します。

USER_CONF を編集するときには、1 行に合計 4096 文字まで入力できます。行は自動的に折り返します。変数の最大長 8192 文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンドディレクティブでは、完全な引数の後にバックスラッシュ（\）行連結文字を使用します。

USER_CONF をリセットすると、空になります。

SNORT_BPF

SNORT_BPF はレガシー拡張変数です。バージョン 5.3.0 以降にアップグレードされる前の旧バージョンの Firepower システム ソフトウェアリリースのときにシステムでこの変数が設定された場合にのみ、これが表示されます。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。

この変数を使用すると、Berkeley Packet Filter（BPF）を適用して、システムに到達する前のトラフィックをフィルタできました。SNORT_BPF に備わっていたフィルタリング機能を今後も適用するには、この変数の代わりにアクセス コントロール ルールを使用してください。この変数は、システム アップグレード前に存在していた設定でのみ表示されます。

変数のリセット

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 *2:* 変数のリセット値

リセットする変数のタイプ	それが含まれるセット タイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	任意
デフォルトまたはユーザ定義	カスタム	現在のデフォルト セット値（変更/未変更にかかわらず）

カスタム セットの変数をリセットすると、単にデフォルト セット内のその変数の現在値にリセットされます。

逆に、デフォルト セットの変数の値をリセットまたは変更すると、すべてのカスタム セット内のその変数のデフォルト値が常に更新されます。リセットアイコンがグレー表示され、その変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタム セット内の変数の値をすでにカスタマイズした場合を除き、デフォルトセットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。

（注） デフォルトセット内の変数を変更するときには、その変更により、リンクされたカスタムセットの変数を使用する侵入ポリシーがどのような影響を受けるか評価するのが適切です（特に、カスタム セット内の変数値をカスタマイズしていない場合）。

変数セット内のリセット アイコン（）の上にポインタを置くと、リセット値を確認できます。カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタム セットまたはデフォルト セットの中で、値 `any` を持つ変数を追加した
- カスタムセットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

セットに変数を追加する

変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。カスタムセットから変数を追加する場合は、設定値をデフォルトセットのカスタマイズ値として使用するかどうかを選択する必要があります。

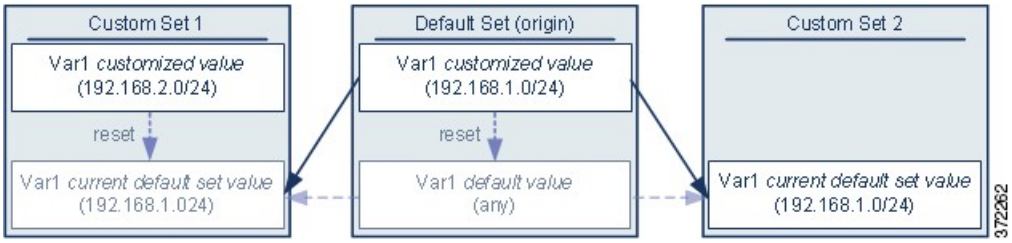
- 設定値（たとえば、192.168.0.0/16）を**使用する**場合、変数は、デフォルト値 `any` を持つカスタマイズ値として設定値を使用するデフォルトセットに追加されます。デフォルトセッ

トの現在の値によって他のセットのデフォルト値が決まるため、他のカスタムセットの初期のデフォルト値は設定値（この例では 192.168.0.0/16）になります。

- 設定値を**使用しない**場合、変数はデフォルト値 `any` のみを使用してデフォルトセットに追加され、こうして、他のカスタム セットの初期のデフォルト値は `any` になります。

例：デフォルト セットへのユーザ定義変数の追加

次の図は、値が `192.168.1.0/24` のデフォルト セットにユーザ定義の変数 `Var1` を追加した場合のセットのインタラクションを示しています。



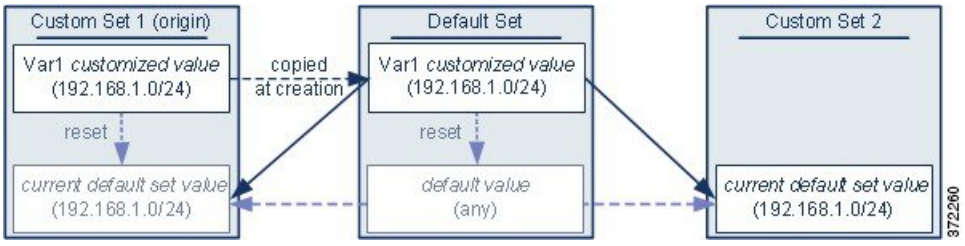
任意のセットで `Var1` の値をカスタマイズできます。`Var1` がカスタマイズされていない Custom Set 2 では、この値は `192.168.1.0/24` です。Custom Set 1 では、`Var1` のカスタマイズ値 `192.168.2.0/24` はデフォルト値をオーバーライドします。デフォルトセットのユーザ定義変数をリセットすると、すべてのセットのそのデフォルト値が `any` にリセットされます。

この例では、Custom Set 2 で `Var1` を更新しなかった場合、デフォルト セットで `Var1` をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 `Var1` が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間のインタラクションは、デフォルトセットのデフォルト変数をリセットすると現在のルール更新で Cisco によって設定された値に、そのデフォルト変数がリセットされること以外は、ユーザ定義変数およびデフォルト変数で同じであることに注意してください。

例：カスタム セットへのユーザ定義変数の追加

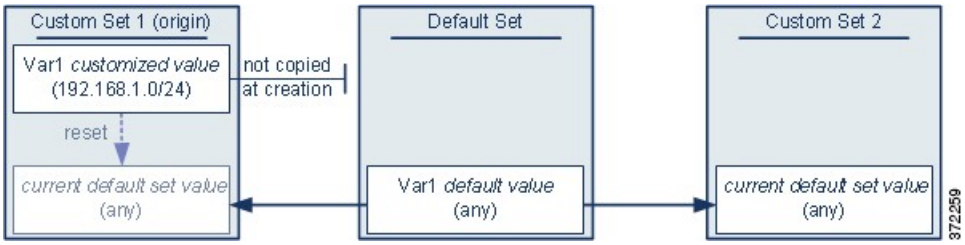
次の 2 つの例は、カスタムセットにユーザ定義変数を追加した場合の変数セットのインタラクションについて示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を**使用する**という選択がなされています。



Custom Set 1 からの `Var1` の発信元を除き、この例は `Var1` をデフォルト セットに追加した上述の例と同じであることに注意してください。`Var1` のカスタマイズ値 `192.168.1.0/24` を Custom

Set 1 に追加すると、値はデフォルト値 any を持つカスタマイズ値としてデフォルト セットにコピーされます。その後、Var1 の値とインタラクションは、Var1 をデフォルト セットに追加した場合と同じになります。前述の例と同様、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の Var1 を Custom Set 1 に追加しますが、Var1 の設定値を他のセットのデフォルト値として**使用しない**ことを選択します。



このアプローチでは、Var1 をデフォルト値 any を持つすべてのセットに追加します。Var1 を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルト セットで Var1 を最初にカスタマイズしないことによって、デフォルト セットの値をカスタマイズし、Var1 をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

変数のネスト

循環したネストにならない限り、変数をネストすることができます。否定形の変数をネストすることはできません。

有効なネストされた変数

以下の例では、SMTP_SERVERS、HTTP_SERVERS、OTHER_SERVERS がネストしても有効な変数です。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

無効なネストされた変数

以下の例では、HOME_NET はネストすると無効な変数です。HOME_NET をネストすると、変数の循環になるためです。つまり、OTHER_SERVERS の定義には HOME_NET が含まれるため、HOME_NET はそれ自体でネストすることになります。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24 HOME_NET	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

ネストでサポートされない否定形の変数

否定形の変数のネストはサポートされないため、以下の例に示されているように、保護ネットワークの外部にある IP アドレスを表す変数 NONCORE_NET を使用することはできません。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	カスタマイズされたデフォルト	—	HOME_NET
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NOT_DMZ_NET	ユーザ定義	—	DMZ_NET
NONCORE_NET	ユーザ定義	EXTERNAL_NET NOT_DMZ_NET	—

ネストでサポートされない否定形の変数の代替手段

上記の例の代替手段として、以下に示す変数 NONCORE_NET を作成することで、保護ネットワークの外部にある IP アドレスを表すことができます。

変数	タイプ（Type）	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NONCORE_NET	ユーザ定義	—	HOME_NET DMZ_NET

変数セットの管理

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）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 変数セットを管理します。

- 追加：カスタムの変数セットを追加するには、[変数セットの追加（Add Variable Set）] をクリックします。変数セットの作成 （41 ページ）を参照してください。
- 削除：カスタムの変数セットを削除するには、変数セットの横にある削除アイコン（）をクリックして、[はい（Yes）] をクリックします。デフォルトの変数セットまたは先祖ドメインに属している変数セットは削除できません。

（注） 削除する変数セットで作成された変数は、別のセットで削除されたり他の方法で影響を受けることはありません。

- 編集：変数セットを編集するには、変更する変数セットの横にある編集アイコン（  ）をクリックします。オブジェクトの編集 （4 ページ）を参照してください。
- フィルタ処理：変数セットを名前でフィルタリングするには、名前の入力を開始します。入力中にページが更新され、一致する名前が表示されます。名前のフィルタリングをクリアするには、フィルタ フィールドにあるクリア アイコン（  ）をクリックします。
- 変数の管理：変数セットに含まれる変数を管理するには、変数の管理 （42 ページ）を参照してください。

変数セットの作成

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 [変数セットの追加（Add Variable Set）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 必要に応じて、[説明（Description）] を入力します。

ステップ 6 セット内の変数を管理します（変数の管理 （42 ページ）を参照）。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

変数の管理

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）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [変数セット（Variable Set）] を選択します。

ステップ 3 編集する変数セットの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 変数を管理します。

- 表示：変数の完全な値を表示するには、変数の横の [値（Value）] 列内の値にポインタを重ねます。
- 追加：変数を追加するには、[追加（Add）] をクリックします。変数の追加 （43 ページ）を参照してください。
- 削除：変数の横にある削除アイコン（  ）をクリックします。変数の追加後に変数セットを保存した場合は、[はい（Yes）] をクリックして、変数の削除を確認します。

  次の変数は削除できません。

  - デフォルトの変数
  - 侵入ルールや別の変数で使用されているユーザ定義変数
  - 先祖ドメインに属している変数

- 編集：編集する変数の横にある編集アイコン（  ）をクリックします。変数の編集 （44 ページ）を参照してください。
- リセット：変更した変数をデフォルト値にリセットするには、変更した変数の横にあるリセット アイコン（  ）をクリックします。リセット アイコンがグレー表示の場合は、次のいずれかが当てはまります。
  - 現在の値がすでにデフォルト値になっている。

- 設定が先祖ドメインに属している。

ヒント アクティブなリセットアイコンの上にポインタを移動して、デフォルト値を表示します。

ステップ 5 [保存（Save）] をクリックして、変数セットを保存します。その変数セットがアクセス コントロール ポリシーで使用されている場合は、[はい（Yes）] をクリックして変更を保存することを確認します。

デフォルト セットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルトセットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

変数の追加

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）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 変数セット エディタで、[追加（Add）] をクリックします。

ステップ 2 [名前（Name）] に一意の変数名を入力します。

ステップ 3 [タイプ（Type）] ドロップダウン リストから、[ネットワーク（Network）] または [ポート（Port）] を選択します。

ステップ 4 変数の値を指定します。

- 使用可能ネットワークまたはポートのリストの項目を包含リストまたは除外リストに移動する場合は、1 つまたは複数の項目を選択してドラッグアンドドロップするか、[包含（Include）] または [除外（Exclude）] をクリックします。

ヒント ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1つのリテラル値を入力し、[追加（Add）]をクリックします。ネットワーク変数の場合、単一のIPアドレスまたはアドレスブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。
- 包含リストまたは除外リストから項目を削除するには、項目の横にある削除アイコン（）をクリックします。

（注） ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ5 [保存（Save）]をクリックして変数を保存します。カスタムセットから新しい変数を追加する場合、次のオプションがあります。

- [はい（Yes）] をクリックすると、設定値を使用する変数がデフォルト セットのカスタマイズ値として追加され、結果として他のカスタムセットのデフォルト値として追加されます。
- [いいえ（No）] をクリックすると、変数はデフォルト セットのデフォルト値 `any` として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

ステップ6 [保存（Save）]をクリックして変数セットを保存します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

変数の編集

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）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

カスタム変数とデフォルト変数の両方を編集できます。

既存の変数の [名前（Name）] と [タイプ（Type）] の値は変更できません。

手順

ステップ 1 変数セット エディタで変更する変数の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 2 変数を変更します。

- 利用可能なネットワークまたはポートのリストから、含める項目のリストまたは除外する項目のリストに項目を移動するには、1 つ以上の項目を選択してからドラッグ アンド ドロップするか、または [含める（Include）] か [除外（Exclude）] をクリックします。

  ヒント ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

- 1 つのリテラル値を入力し、[追加（Add）] をクリックします。ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。
- 含めるリストまたは除外リストから項目を削除するには、項目の横にある削除アイコン（  ）をクリックします。

（注） ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

ステップ 3 [保存（Save）] をクリックして変数を保存します。

ステップ 4 [保存（Save）] をクリックして変数セットを保存します。変数セットがアクセス コントロール ポリシーで使用されている場合、[はい（Yes）] をクリックして変更の保存を確認します。変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

セキュリティ インテリジェンスのリストとフィード

セキュリティ インテリジェンスのリストとフィードは、以下を収集することでトラフィックをすばやくフィルタリングするのに役立ちます。

- IP アドレスとアドレス ブロック：アクセス コントロール ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。
- ドメイン名：DNS ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。
- URL：アクセス コントロール ポリシーでセキュリティ インテリジェンスの一部としてブラックリスト化およびホワイトリスト化するのに使用します。また、セキュリティ インテリジェンス後に分析およびトラフィック処理フェーズが実行されるアクセス コントロール ルールおよび QoS ルールで、URL リストを使用することもできます。

一覧

リストは、手動で管理される静的コレクションです。

デフォルトで、アクセス コントロール ポリシーと DNS ポリシーは、セキュリティ インテリジェンスの一部としてグローバル ブラックリストおよびホワイトリストを使用します。[今すぐホワイトリストに登録（Whitelist Now）] および [今すぐブラックリストに登録（Blacklist Now）] アクションを使用することで、再展開することなくセキュリティ インテリジェンス リストを作成して実装できます。[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト （48 ページ）を参照してください。

カスタム リストは、フィードやグローバル リストを増補および微調整できます。ただし、カスタム リストを実装するには再展開する必要があります。

フィード

フィードは、HTTP または HTTPS で一定期間更新する動的コレクションです。

定期的に更新される Cisco Intelligence Feed を使用すると、Talos からの最新の脅威インテリジェンスに基づいてネットワーク トラフィックをフィルタリングできます。また、サードパーティのフィードを使用することもできます。あるいは、カスタム内部フィードを使用すると、複数の Firepower Management Center からなる大規模な導入で企業全体のブラックリストを簡単に保守できます。

システムがフィードを更新する際は、変更が伝搬されるまで数分かかりますが、再展開の必要はありません。システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にすることができます。ただし、自動更新を行えば、最新の関連するデータであることが確実になります。

（注） システムはカスタム フィードのダウンロード時にピア SSL 証明書の検証を実行**しません**。また、システムは、証明書のバンドルまたは自己署名証明書を使用したリモート ピアの検証もサポートしていません。

リストとフィードの書式設定

各リストまたはフィードは、500MB 未満の単純なテキスト ファイルでなければなりません。リスト ファイルの拡張子は .txt でなければなりません。1 行につきエントリまたはコメントを 1 つ（IP アドレス 1 つ、URL 1 つ、ドメイン名 1 つ）含めます。

ヒント　含めることができるエントリの数は、ファイルの最大サイズによって制限されます。たとえば、コメントがなくURLの長さの平均が100文字（PunycodeまたはUnicode表現と改行のパーセントを含む）の URL リストには、524 万を超えるエントリを含めることができます。

DNSリストエントリ内では、ドメインラベルとしてアスタリスク（*）ワイルドカード文字を指定できます。その場合、すべてのラベルがワイルドカードと一致します。たとえば、`www.example.*` のエントリは `www.example.com` と `www.example.co` の両方に一致します。

ソース ファイル内にコメント行を含める場合は、シャープ（#）文字で開始する必要があります。コメントが含まれるソースファイルをアップロードすると、システムによってアップロード中にコメントが削除されます。ダウンロードするソースファイルには、コメントを除くすべてのエントリが含まれます。

システムが破損したフィードまたは認識不能なエントリがあるフィードをダウンロードした場合、システムは古いフィードデータを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内のエントリを1つでも認識できる場合、システムは認識できるエントリを使用します。

セキュリティ インテリジェンス オブジェクトのクイック リファレンス

オブジェクト タイプ（Object Type）	機能の編集	編集後に再度展開しますか?
デフォルト（カスタム入力）ホワイトリストとブラックリスト：グローバル、子孫、ドメイン固有	コンテキスト メニューを使用してエントリを追加。 オブジェクト マネージャを使用してエントリを削除。	エントリを追加後、いいえ。 エントリを削除後、はい。
カスタム ホワイトリストとブラックリスト	オブジェクト マネージャを使用して新しいリストと交換リストをアップロード。	○
システム提供インテリジェンス フィード	オブジェクト マネージャを使用して更新頻度を無効または変更。	なし
カスタム フィード	オブジェクト マネージャを使用して完全に変更。	なし

オブジェクト タイプ（Object Type）	機能の編集	編集後に再度展開しますか?
シンクホール	オブジェクト マネージャを使用して完全に変更。	○

[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト

Firepower Management Center のコンテキスト メニュー（コンテキスト メニューを参照）では、セキュリティ インテリジェンスを使って、すばやくブラックリストやホワイトリストに登録することができます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気付いた場合、それらの IP アドレスを即座にブラックリストに入れることができます。変更内容が伝達されるまでに数分かかる場合がありますが、再度展開する必要はありません。

[今すぐブラックリストに登録（Blacklist Now）] と [今すぐホワイトリストに登録（Whitelist Now）] のコンテキスト メニュー オプションは、IP アドレス、URL、DNS 要求ホットスポットに使用可能です。コンテキスト メニューでブラックリストまたはホワイトリストに登録すると、選択した項目が該当するデフォルト グローバル リストに追加されます。デフォルトでは、アクセス コントロール ポリシーと DNS ポリシーがすべてのセキュリティ ゾーンに適用されるグローバル リストを使用します。ポリシーごとに、これらのリストを使用しないように選択することができます。

（注） これらのオプションは、セキュリティ インテリジェンスにのみ適用されます。セキュリティ インテリジェンスは、すでにファーストパスされたトラフィックをブラックリストに登録することはできません。同様に、セキュリティ インテリジェンスでホワイトリストに登録しても、それに一致するトラフィックが自動的に信頼されることもファーストパスされることもありません。詳細については、セキュリティ インテリジェンスについてを参照してください。

コンテキスト メニュー オプション	対象項目	対象グローバル リスト
[今すぐブラックリストに追加（Blacklist Now）] [今すぐホワイトリストに追加（Whitelist Now）]	IP アドレス	[グローバル ブラックリスト（Global Blacklist）] [グローバル ホワイトリスト（Global Whitelist）]

コンテキスト メニュー オプション	対象項目	対象グローバル リスト
[今すぐ URL に HTTP/S 接続をブラックリストする（Blacklist HTTP/S Connections to URL Now）] [今すぐ URL に HTTP/S 接続をホワイトリストする（Whitelist HTTP/S Connections to URL Now）]	URL	[URL グローバル ブラックリスト（Global Blacklist for URL）] [URL グローバル ホワイトリスト（Global Whitelist for URL）]
[今すぐドメインに HTTP/S 接続をブラックリストする（Blacklist HTTP/S Connections to Domain Now）] [今すぐドメインに HTTP/S 接続をホワイトリストする（Whitelist HTTP/S Connections to Domain Now）]	ドメイン全体	[URL グローバル ブラックリスト（Global Blacklist for URL）] [URL グローバル ホワイトリスト（Global Whitelist for URL）]
[今すぐドメインに DNS 要求をブラックリストする（Blacklist DNS Requests to Domain Now）] [今すぐドメインに DNS 要求をホワイトリストする（Whitelist DNS Requests to Domain Now）]	ドメイン全体の DNS 要求	[DNS グローバル ブラックリスト（Global Blacklist for DNS）] [DNS グローバル ホワイトリスト（Global Whitelist for DNS）]

マルチドメイン展開では、グローバル リストだけでなくドメイン リストにも項目を登録することで、ブラックリストやホワイトリストを適用する Firepower システム ドメインを選択することができます。セキュリティ インテリジェンス リストとマルチテナンシー（49 ページ）を参照してください。

セキュリティ インテリジェンス リストにエントリを追加すると、アクセス制御に影響が出るため、次のうちいずれか 1 つが必須です。

- 管理者（Administrator）アクセス
- デフォルト ロールの組み合わせ：ネットワーク管理者（Network Admin）またはアクセス管理者（Access Admin）に加えてセキュリティ アナリスト（Security Analyst）およびセキュリティ承認者（Security Approver）
- アクセス コントロール ポリシーの変更（Modify Access Control Policy）と設定をデバイスに展開（Deploy Configuration to Devices）の両方のアクセス許可を持つカスタム ロール。

セキュリティ インテリジェンス リストとマルチテナンシー

マルチドメイン展開では、グローバル ドメインは、グローバルなブラックリストとホワイトリストを所有しています。グローバル リストに対して項目を追加または削除できるのは、グローバル管理者のみです。サブドメイン ユーザがネットワーク、ドメイン名、および URL をホワ

イトリストとブラックリストに追加できるように、マルチテナンシーでは次のものが追加されます。

- ドメイン リスト：コンテンツが特定のサブドメインにのみ適用されるホワイトリストまたはブラックリスト。グローバル リストは、グローバル ドメインのドメイン リストです。
- 子孫ドメイン リスト：現在のドメインの子孫のドメイン リストを集約するホワイトリストまたはブラックリスト。

ドメイン リスト

グローバルリストに（編集ではなく）アクセスできることに加えて、各サブドメインには独自の名前付きリストがあり、そのコンテンツはそのサブドメインにのみ適用されます。たとえば、Company A という名前のサブドメインは、次のリストを所有するとします。

- ドメイン ブラックリスト - Company A およびドメイン ホワイトリスト - Company A
- DNS のドメイン ブラックリスト - Company A、および DNS のドメイン ホワイトリスト - Company A
- URL のドメイン ブラックリスト - Company A、および URL のドメイン ホワイトリスト - Company A

現在のドメインより上位の管理者は、これらのリストに入力できます。コンテキストメニューを使用して、現在のドメインとすべての子孫ドメインの項目をブラックリストまたはホワイトリストに追加できます。ただし、ドメインリストから項目を削除できるのは、関連付けられたドメインの管理者のみです。

たとえば、グローバル管理者はグローバル ドメインと Company A のドメインの同じ IP アドレスをブラックリストに追加できますが、それを Company B のドメインのブラックリストには追加できません。このアクションにより、同じ IP アドレスが次のリストに追加されます。

- （グローバル管理者のみが削除できる）グローバル ブラックリスト
- （Company A の管理者のみが削除できる）ドメインブラックリスト- Company A

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

子孫ドメイン リスト

子孫ドメイン リストは、現在のドメインの子孫のドメイン リストを集約するホワイトリストまたはブラックリストです。リーフ ドメインには、子孫ドメイン リストはありません。

子孫ドメイン リストが便利なのは、上位レベルのドメインの管理者が一般的なセキュリティ インテリジェンス設定を適用できる一方で、サブドメインユーザは独自の展開で項目をブラックリストやホワイトリストに追加できるためです。

たとえば、グローバル ドメインには、次の子孫ドメイン リストがあります。

- 子孫ブラックリスト - グローバルおよび子孫のホワイトリスト - グローバル

- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル
- URL の子孫ブラックリスト - グローバル、および子孫の URL のホワイトリスト - グローバル

（注） 子孫ドメインリストは、手動で入力されたリストではなく象徴的な集約であるため、オブジェクト マネージャには表示されません。それを使用できる場所、つまり、アクセス コントロール ポリシーと DNS ポリシーに表示されます。

セキュリティ インテリジェンス フィードの更新頻度の変更

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**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

システムが提供するフィードは削除できませんが、更新頻度を変更（または無効に設定）できます。デフォルトで、フィードは 2 時間ごとに更新されます。

マルチドメイン展開では、システムが提供するフィードはグローバルドメインに属し、このドメインの管理者のみが変更できます。ユーザは、各自が使用するドメインに属するカスタム フィードの更新頻度を更新できます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、更新頻度を変更するフィードのタイプを選択します。

ステップ 3 更新するフィードの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [更新頻度（Update Frequency）] を編集します。

ステップ 5 [保存（Save）] をクリックします。

カスタム セキュリティ インテリジェンス フィード

カスタムまたはサードパーティのセキュリティ インテリジェンス フィードを使用すると、インターネット上で定期的に更新される他の信頼できるホワイトリストおよびブラックリストによって、システムが提供するインテリジェンスフィードを拡張することができます。内部フィードをセットアップすることもできます。これは、1つのソースリストを使用して導入環境で複数の Firepower Management Center を更新する場合に役立ちます。

（注） セキュリティ インテリジェンス フィードでは、/0 ネットマスクを使ってアドレス ブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ（Monitor）] または [ブロック（Block）] ルール アクションを含むアクセス コントロール ルールを使用し、デフォルト値 any を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode によりエンコードできません。デフォルトで、システムは設定した間隔でフィード ソース全体をダウンロードし、管理対象デバイスを自動更新します。

md5 チェックサムを使用して、更新フィードをダウンロードするかどうか判断するようにシステムを設定することもできます。システムが最後にフィードをダウンロードした後にチェックサムが変更されていない場合、再ダウンロードする必要はありません。特に内部フィードが大きい場合には、md5 チェックサムを使用することができます。md5 チェックサムは、チェックサムのみを含む単純なテキスト ファイルに保存する必要があります。コメントはサポートされていません。

手動でセキュリティ インテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

セキュリティ インテリジェンス フィードの作成

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**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、追加するフィード タイプを選択します。

ステップ 3 上記で選択したフィード タイプに適したオプションをクリックします。

- **[ネットワーク リストとフィードの追加（Add Network Lists and Feeds）]**
- **[DNS リストとフィードの追加（Add DNS Lists and Feeds）]**
- **[URL リストとフィードの追加（Add URL Lists and Feeds）]**

ステップ 4 フィードの名前を [名前（Name）] に入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [タイプ（Type）] ドロップダウンリストから [フィード（Feed）] を選択します。

ステップ 6 [フィード URL（Feed URL）] を入力します。

ステップ 7 オプションで、[MD5 URL] を入力します。

ステップ 8 [更新頻度（Update Frequency）] を選択します。

ステップ 9 [保存（Save）] をクリックします。
フィードの更新を無効にした場合を除き、システムはフィードをダウンロードして検証しようとします。

手動によるセキュリティ インテリジェンス フィードの更新

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**）
脅威（セキュリティ インテリジェンス）	保護（セキュリティ インテリジェンス）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、フィード タイプを選択します。

ステップ 3 [フィードの更新（Update Feeds）] をクリックして、確認します。

ステップ 4 [OK] をクリックします。

フィードの更新をダウンロードして検証した後、Firepower Management Center はすべての変更内容を管理対象デバイスに通知します。導入環境では、更新されたフィードを使用してトラフィックのフィルタリングが開始されます。

カスタム セキュリティ インテリジェンス リスト

セキュリティ インテリジェンス リストは、IP アドレス、アドレス ブロック、URL、またはドメイン名の単純なスタティック リストで、ユーザがシステムに手動でアップロードします。カスタム リストは、単一の Firepower Management Center の管理対象デバイスで、フィードやグローバル リストの 1 つを増やしたり、微調整したりする場合に役立ちます。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしているものの、このフィードが全体的に部門にとって有用である場合、IP アドレス フィード オブジェクトをアクセス コントロール ポリシーのブラックリストから削除する代わりに、誤って分類された IP アドレスだけが含まれるカスタム ホワイトリストを作成できます。

（注） セキュリティ インテリジェンス リストでは、`/0` ネットマスクを使ってアドレス ブロックをホワイトリスト登録またはブラックリスト登録することはできません。ポリシーですべてのトラフィックをモニタまたはブロックする場合は、[モニタ（Monitor）] または [ブロック（Block）] ルール アクションを含むアクセス コントロール ルールを使用し、デフォルト値 `any` を [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに設定します。

リスト エントリのフォーマットについて、次の点に注意してください。

- アドレス ブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ `0` から `32`、または `0` から `128` までの整数になります。
- ドメイン名に含まれる Unicode は Punycode 形式でエンコードされる必要があります。大文字と小文字は区別されません。
- ドメイン名の文字の大文字と小文字は区別されません。
- URL に含まれる Unicode はパーセントエンコーディング形式でエンコードする必要があります。
- URL サブディレクトリの文字の大文字と小文字は区別されます。
- シャープ記号（`#`）で始まるリスト エントリは、コメントと見なされます。

リスト エントリの照合について、次の点に注意してください。

- URL または DNS リストにより高位レベルのドメインが存在する場合、システムはそれより低いレベルのドメインを一致とします。たとえば、DNS リストに `example.com` を追加すると、システムは `www.example.com` と `test.example.com` の両方を一致とします。
- システムは DNS または URL リスト エントリに対して DNS ルックアップを（フォワード ルックアップ、リバース ルックアップともに）行いません。たとえば、URL リストに `http://192.168.0.2` を追加し、これがルックアップすれば `http://www.example.com` であったとします。この場合、システムは `http://192.168.0.2` のみ一致とし、`http://www.example.com` は一致となりません。

- URL リストに末尾がスラッシュ（/）記号で終わる URL を追加した場合、そのエントリに一致するのは完全に一致する URL のみとなります。
- URL または DNS リストに末尾にスラッシュ記号のない URL を追加した場合、そのエントリと同じプレフィックスを持つ URL は一致となります。たとえば、URL リストに `www.example.com` を追加すると、システムは `www.example.com` と `www.example.com/example` の両方を一致とします。

新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロード

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

セキュリティ インテリジェンス リストを変更するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があります。Web インターフェイスを使用してファイルの内容を変更することはできません。ソース ファイルへのアクセス権がない場合は、システムからコピーをダウンロードします。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 上記の手順で選択したリストに該当するオプションをクリックします。

- **[ネットワーク リストとフィードの追加（Add Network Lists and Feeds）]**
- **[DNS リストとフィードの追加（Add DNS Lists and Feeds）]**
- **[URL リストとフィードの追加（Add URL Lists and Feeds）]**

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [タイプ（Type）] ドロップダウン リストから、[リスト（List）] を選択します。

ステップ 6 [参照（Browse）] をクリックしてリストの `.txt` ファイルを位置指定し、[アップロード（Upload）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

セキュリティ インテリジェンス リストの更新

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）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [セキュリティ インテリジェンス（Security Intelligence）] ノードを展開し、リストのタイプを選択します。

ステップ 3 更新するリストの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 編集するリストのコピーが必要な場合、[ダウンロード（Download）]をクリックし、ブラウザのプロンプトに従ってリストをテキスト ファイルとして保存します。

ステップ 5 必要に応じてリストを変更します。

ステップ 6 [セキュリティ インテリジェンス（Security Intelligence）] ポップアップ ウィンドウで、[参照（Browse）]をクリックして、変更されたリストを参照し、[アップロード（Upload）]をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

シンクホール オブジェクト

シンクホール オブジェクトとは、シンクホール内のすべてのドメイン名のルーティング不可アドレスか、またはサーバに解決されない IP アドレスのいずれかを付与する DNS サーバを表します。DNS ポリシー ルール内のシンクホール オブジェクトを参照して、一致するトラフィックをシンクホールにリダイレクトすることができます。オブジェクトには、IPv4 アドレスと IPv6 アドレスの両方を割り当てる必要があります。

シンクホール オブジェクトの作成

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**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [シンクホール（Sinkhole）] を選択します。

ステップ 3 [シンクホールの追加（Add Sinkhole）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 シンクホールの [IPv4 アドレス（IPv4 Address）] と [IPv6 アドレス（IPv6 Address）] を入力します。

ステップ 6 次の選択肢があります。

- シンクホール サーバへのトラフィックをリダイレクトする場合は、[シンクホールへの接続のログ（Log Connections to Sinkhole）] を選択します。
- 非解決 IP アドレスにトラフィックをリダイレクトする場合は、[シンクホールへの接続をブロックしてログ（Block and Log Connections to Sinkhole）] を選択します。

ステップ 7 侵入の痕跡（IoC）のタイプをシンクホールに割り当てるには、[タイプ（Type）] ドロップダウンからいずれかのタイプを選択します。

ステップ 8 [保存（Save）] をクリックします。

ファイル リスト

AMP for Firepowerを使用しており、AMPクラウドがファイルの性質を誤って特定した場合は、このファイルをファイル リストに追加して、今後さらに検出できます。このファイルは、SHA-256 ハッシュ値を使用して指定されます。各ファイル リストには、一意の SHA-256 値を最大 10000 個まで含めることができます。

ファイル リストには 2 種類の事前定義済みカテゴリがあります。

クリーン リスト

このリストにファイルを追加すると、システムは AMP クラウドがクリーンな性質を割り当てた場合と同様にファイルを扱います。

カスタム検出リスト

このリストにファイルを追加すると、システムは AMP クラウドがマルウェアの性質を割り当てた場合と同様にファイルを扱います。

マルチドメイン展開では、各ドメインにクリーン リストとカスタム検出リストが存在します。下位レベルのドメインでは、先祖のリストを表示できますが、変更できません。

これらのリストに含まれているファイルに手動でブロッキング動作を指定するため、システムはこれらのファイルの性質についてAMPクラウドに照会しません。ファイルのSHA値を計算するには、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションと [マルウェア ブロック（Block Malware）] アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があります。

⚠

注意 クリーン リストにマルウェアを**含めない**でください。クリーン リストによって、AMP クラウドおよびカスタム検出リストの両方がオーバーライドされます。

ファイル リストのソース ファイル

SHA-256 値のリストと説明を含むコンマ区切り値（CSV）ソース ファイルをアップロードすることによって、複数のSHA-256値をファイル リストに追加できます。Firepower Management Center はその内容を検証し、有効な SHA-256 値をファイル リストに入れます。

ソース ファイルは、ファイル名拡張子 .csv の単純なテキスト ファイルである必要があります。見出しはポンド記号（#）で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1 つの SHA-256 値の後に説明が含まれる必要があり、LF または CR+LF 改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべての SHA-256 ハッシュもファイル リストから削除されます。

- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイル リストに含まれる場合は、複数のファイルをファイル リストにアップロードすることはできません。
- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にコンマを含める場合は、エスケープ文字（\）を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。
- 重複しないすべての SHA-256 値がこのファイル リストに追加されます。すでにファイル リストに存在する SHA-256 値を含むソース ファイルをアップロードした場合、新しくアップロードされた値によって既存の SHA--256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイル イベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。
- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。
- アップロードされた複数のソース ファイル内に同じ SHA--256 値に関するエントリが含まれる場合、システムは最も新しい値を使用します。
- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソースファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。
- ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイル リストからソース ファイルを削除すると、ファイル リストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

ファイル リスト別の SHA-256 値の追加

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）
マルウェア	マルウェア	Firepower	任意（Any）	Admin/Network Admin/Access Admin

ファイルの SHA-256 値を送信して、それをファイル リストに追加できます。重複する SHA-256 値は追加できません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

始める前に

- イベント ビューからファイルまたはマルウェア イベントを右クリックし、コンテキスト メニューで [フル テキストの表示（Show Full Text）] を選択し、ファイルの SHA-256 値全体をコピーし、ファイルリストに貼り付けます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加元（Add by）] ドロップダウンリストから [SHA 値の入力（Enter SHA Value）] を選択します。

ステップ 5 [説明（Description）] フィールドにソース ファイルの説明を入力します。

ステップ 6 [SHA-256] フィールドにファイル全体の値を入力し、または貼り付けます。システムでは値の部分的な一致はサポートされません。

ステップ 7 [追加（Add）] 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

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストへの個々のファイルのアップロード

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**）
マルウェア	マルウェア	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルを Firepower Management Center にアップロードできます。システムはファイルの SHA-256 値を計算し、ファイルをリストに追加します。SHA-256 を計算するとき、システムはファイル サイズを制限しません。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加（Add by）] ドロップダウン リストから、[SHA の計算（Calculate SHA）] を選択します。

ステップ 5 オプションで、[説明（Description）] フィールドにファイルの説明を入力します。説明を入力しない場合、アップロード時にファイル名が説明として使用されます。

ステップ 6 [参照（Browse）] をクリックし、アップロードするファイルを選択します。

ステップ 7 [SHA の計算と追加（Calculate and Add SHA）] 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

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

（注） 設定の変更を導入すると、その後システムはそのリストのファイルを AMP クラウドでクエリしなくなります。

ファイル リストへのソース ファイルのアップロード

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**）
マルウェア	マルウェア	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ソース ファイルからの値の追加先となるファイル リストの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 [追加方法（**Add by**）] ドロップダウン リストで [SHA のリスト（List of SHAs）] を選択します。

ステップ 5 オプションで、[説明（Description）] フィールドにソース ファイルの説明を入力します。説明を入力しない場合、システムはファイル名を使用します。

ステップ 6 [参照（Browse）] をクリックしてソース ファイルを参照してから、[リストのアップロードと追加（Upload and Add List）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

（注） ポリシーを展開したら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストの SHA-256 値の編集

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）
マルウェア	マルウェア	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

ファイル リストの個々の SHA-256 値を編集または削除することができます。オブジェクト マネージャ内でソース ファイルを直接編集できないことに注意してください。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [ファイル リスト（File List）] をクリックします。

ステップ 3 ファイルの変更対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 次の操作を実行できます。

- 変更する SHA-256 値の横にある編集アイコン（）をクリックし、必要に応じて [SHA-256] または [説明（Description）] の値を変更します。
- 削除する SHA-256 値の横にある削除アイコン（）をクリックします。

ステップ 5 [保存（Save）] をクリックし、リストのファイル エントリを更新します。

ステップ 6 [保存（Save）] をクリックして、ファイル リストを保存します。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

（注） 設定の変更が展開されたら、システムはそのリストのファイルについて AMP クラウドに問い合わせなくなります。

ファイル リストからのソース ファイルのダウンロード

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**）
マルウェア	マルウェア	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクト タイプのリストから [ファイル リスト（File List）] を選択します。

ステップ 3 ソース ファイルのダウンロード対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、オブジェクトは先祖ドメインに属しており、オブジェクトを変更する権限がありません。

ステップ 4 ダウンロードするソース ファイルの横にある表示アイコン（）をクリックします。

ステップ 5 [SHA リストのダウンロード（Download SHA List）] をクリックし、プロンプトに従ってソース ファイルを保存します。

ステップ 6 [閉じる（Close）] をクリックします。

暗号スイート リスト

暗号スイート リストは複数の暗号スイートからなるオブジェクトです。定義済み暗号スイートの値は、SSL または TLS 暗号化セッションのネゴシエートに使われる暗号スイートを表しています。暗号スイートおよび暗号スイート リストを SSL ルールで使用すると、クライアントとサーバが暗号スイートを使って SSL セッションをネゴシエートしたかどうかに基づいて暗号化

トラフィックを制御できます。SSLルールに暗号スイートリストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされたSSLセッションがルールに一致します。

（注） Webインターフェイスでは暗号スイートリストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

暗号スイート リストの作成

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 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ2 オブジェクト タイプのリストから [暗号スイート リスト（Cipher Suite List）] を選択します。

ステップ3 [暗号スイートの追加（Add Cipher Suites）] をクリックします。

ステップ4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ5 [使用可能な暗号（Available Ciphers）] リストから、1つ以上の暗号スイートを選択します。

ステップ6 [追加（Add）] をクリックします。

ステップ7 オプションで、[選択された暗号（Selected Ciphers）] リストで、削除する暗号スイートの隣にある削除アイコン（）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

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

識別名オブジェクト

それぞれの識別名オブジェクトは、公開鍵証明書のサブジェクトまたは発行元にリストされた識別名を表します。SSLルールで識別名オブジェクトとグループを使用すると、サブジェクトまたは発行元として識別名を含むサーバ証明書を使ってクライアントとサーバがSSLセッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

識別名オブジェクトには、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、システムはオブジェクトを保存する前に「CN=」を追加します。

さらに、次の表に示す属性を含む識別名を追加することもできます。属性はカンマで区切って使用します。

表 *3:* 識別名の属性

属性（Attribute）	説明	使用可能な値
C	国コード（Country Code）	2 つの英字
CN	Common Name	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
O	Organization	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
OU	組織	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字

ワイルドカードとして1つ以上のアスタリスク（*）を属性に定義できます。共通名属性では、ドメイン名ラベルごとに1つ以上のアスタリスクを定義できます。ワイルドカードはそのラベル内でのみ照合されますが、ワイルドカードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 *4:* 共通名属性のワイルドカードの例

属性（Attribute）	一致	一致しない
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com

属性（**Attribute**）	一致	一致しない
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

識別名オブジェクトの作成

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 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [識別名（Distinguished Name）] ノードを展開し、[個別オブジェクト（Individual Objects）] を選択します。

ステップ 3 [識別名の追加（Add Distinguished Name）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、識別名オブジェクト （66 ページ）に示されている属性をカンマで区切って含めることができます。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

PKI オブジェクト

SSL アプリケーションの PKI オブジェクト

PKI オブジェクトは、導入をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局（CA）証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバ証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。

信頼できる認証局オブジェクトと内部証明書オブジェクトを使用して ISE/ISE-PIC への接続を設定する場合、ISE/ISE-PIC をアイデンティティ ソースとして使用できます。

内部証明書オブジェクトを使用してキャプティブ ポータルを設定する場合、システムはキャプティブ ポータル デバイスがユーザの Web ブラウザに接続する際に、デバイスのアイデンティティを検証できます。

信頼できる認証局オブジェクトを使用してレルムを設定する場合、LDAP または AD サーバへのセキュア接続を設定できます。

SSL ルールで PKI オブジェクトを使用する場合、以下のものを使用して暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

SSL ルールで PKI オブジェクトを使用する場合、以下のものを復号できます。

- 発信トラフィック：内部 CA オブジェクトを使ってサーバ証明書を再署名することによって復号します
- 受信トラフィック：内部証明書オブジェクトにある既知の秘密鍵を使用して復号します

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、システムは証明書のサブジェクト識別名をオブジェクト値として表示します。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。証明書に関する他の詳細を表示するには、PKI オブジェクトを編集します。

（注） Firepower Management Center および管理対象デバイスは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密キーを、保存前にランダムに生成されたキーを使って暗号化します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使って秘密キーを復号し、ランダムに生成されたキーを使ってそれを再暗号化してから保存します。

証明書の登録の PKI オブジェクト

証明書の登録オブジェクトには、証明書署名要求（CSR）を作成したり、指定された CA からアイデンティティ証明書を取得したりするために必要な証明機関（CA）サーバ情報や登録パラメータが含まれています。これらのアクティビティは、秘密キー インフラストラクチャ（PKI）で発生します。

証明書の登録オブジェクトには、証明書失効情報も含まれている場合があります。PKI、デジタル証明書、および証明書の登録の詳細については、PKI インフラストラクチャとデジタル証明書 を参照してください。

内部認証局オブジェクト

設定されたそれぞれの内部認証局（CA）オブジェクトは、組織で制御される CA の CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA 証明書、およびペアになった秘密鍵からなります。SSL ルールで内部 CA オブジェクトとグループを使用すると、内部 CA によってサーバ証明書に再署名することにより、発信する暗号化トラフィックを復号できます。

（注） [復号 - 再署名（Decrypt - Resign）] SSL ルールで内部 CA オブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSL ハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメイン リストに内部CA オブジェクト証明書を追加します。

次の方法で内部 CA オブジェクトを作成できます。

- RSA ベースまたは楕円曲線ベースの既存の CA 証明書と秘密キーをインポートする
- 新しい RSA ベースの自己署名 CA 証明書と秘密キーを生成する

- RSA ベースの未署名の CA 証明書と秘密キーを生成する内部 CA オブジェクトを使用する前に、証明書に署名するために証明書署名要求（CSR）を別の CA に送信する必要があります。

署名付き証明書を含む内部CAオブジェクトを作成した後で、CA証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システムで生成された場合でも、ユーザによって作成された場合でも、内部CAオブジェクトの名前は変更できますが、他のオブジェクト プロパティは変更できません。

使用中の内部 CA オブジェクトは削除できません。さらに、SSL ポリシーで使用される内部CAオブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

CA 証明書と秘密キーのインポート

X.509 v3 CA 証明書と秘密キーをインポートすることによって、内部 CA オブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

秘密キーファイルがパスワード保護されている場合は、復号パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

（注） ルールに [復号 - 再署名（Decrypt - Resign）] アクションを設定すると、そのルールでは、設定されているルール条件に加えて、参照される内部CA証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号するには、楕円曲線ベースのCA証明書をアップロードする必要があります。

CA 証明書と秘密キーのインポート

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開して、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA のインポート（Import CA）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロード ファイルがパスワード保護されている場合は、[暗号化および次のパスワード:（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

CA 証明書および秘密キーの生成

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

識別情報を提供することで、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。

生成される CA 証明書の有効期間は 10 年です。[有効期間の開始（Valid From）] の日付は、生成の一週間前です。

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA の生成（Generate CA）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 ID 属性を入力します。

ステップ 6 [自己署名 CA の生成（Generate self-signed CA）] をクリックします。

新しい署名付き証明書

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求（CSR）が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できます。

未署名の CA 証明書と CSR の作成

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 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 [CA の生成（Generate CA）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 ID 属性を入力します。

ステップ 6 [CSR の作成（Generate CSR）] をクリックします。

ステップ 7 CA に送信するために CSR をコピーします。

ステップ 8 [OK] をクリックします。

次のタスク

- CA によって発行される署名済み証明書をアップロードする必要があります。次のページを参照してください。 CSR への応答として発行された署名付き証明書のアップロード （73 ページ）

CSR への応答として発行された署名付き証明書のアップロード

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

一度アップロードすると、署名付き証明書は SSL ルールで参照できます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 CSR を待機している未署名の証明書を含む CA オブジェクトの横の編集アイコン（  ）をクリックします。

ステップ 4 [証明書のインストール（Install Certificate）] をクリックします。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 アップロード ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェック ボックスをオンにして、パスワードを入力します。

ステップ 7 [保存（Save）] をクリックして、CA オブジェクトに署名付き証明書をアップロードします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

CA 証明書および秘密キーのダウンロード

証明書および鍵の情報を含むファイルを内部 CA オブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。

注意 ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロードファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。

注意 システム バックアップの一部としてダウンロードされる秘密鍵は、復号されてから、非暗号化バックアップ ファイルに保存されます。

CA 証明書と秘密キーのダウンロード

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

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほ

とんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

現在のドメインおよび先祖ドメインの両方の CA 証明書をダウンロードできます。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部 CA（Internal CAs）] を選択します。

ステップ 3 証明書および秘密キーをダウンロードする対象となる内部 CA オブジェクトの横の編集アイコン（）をクリックします。

マルチドメイン導入では、表示アイコン（）をクリックして、先祖ドメインのオブジェクトの証明書および秘密キーをダウンロードします。

ステップ 4 [ダウンロード（Download）] をクリックします。

ステップ 5 [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに、暗号化パスワードを入力します。

ステップ 6 [OK] をクリックします。

信頼できる認証局オブジェクト

設定した信頼できる認証局（CA）オブジェクトは、それぞれ信頼できる CA に属する CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名と CA 公開鍵証明書からなります。次のものに設定された外部 CA オブジェクトとグループを使用できます。

- 信頼できる CA、または信頼チェーン内のいずれかの CA によって署名された証明書で暗号化されたトラフィックを制御するための SSL ポリシー。
- LDAP または AD サーバへのセキュアな接続を確立するためのレルムの設定。
- ISE/ISE-PIC 接続。[pxGrid サーバ CA（pxGrid Server CA）] フィールドと [MNT サーバ CA（MNT Server CA）] フィールドで信頼できる認証局オブジェクトを選択します。

信頼できる CA オブジェクトを作成した後で、その名前を変更したり、証明書失効リスト（CRL）を追加したりすることはできますが、他のオブジェクトプロパティを変更することはできません。オブジェクトに追加できる CRL の数には制限がありません。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

（注） オブジェクトに CRL を追加しても、オブジェクトが ISE/ISE-PIC 統合設定で使用される場合は効果がありません。

使用中の信頼できる CA オブジェクトを削除することはできません。また、使用中の信頼できる CA オブジェクトを編集すると、関連付けられているアクセス コントロール ポリシーが最新ではなくなります。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

信頼できる CA オブジェクト

外部 CA オブジェクトは、X.509 v3 CA 証明書をアップロードすることによって設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワードで保護されている場合は、復号パスワードを提供する必要があります。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA 証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

信頼できる CA オブジェクトの追加

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）	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 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3 [信頼できる CA の追加（Add Trusted CAs）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 ファイルがパスワード保護されている場合は、[暗号化、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

信頼できる CA オブジェクトの証明書失効リスト

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

CRL を追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切な CRL を含んでいるファイルのみをアップロードできます。信頼できる CA オブジェクトに追加できる CRL の数には制限がありません。ただし、CRL をアップロードした場合、別の CRL を追加する前に、オブジェクトをその都度保存する必要があります。

（注） オブジェクトが ISE/ISE-PIC 統合設定で使用されている場合は、オブジェクトに CRL を追加しても影響はありません。

信頼できる CA オブジェクトへの証明書失効リストの追加

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）	任意（Any）	すべて（NGIPSv を除く）	任意（Any）	Admin/Access Admin/Network Admin

マルチドメインの展開では、現在のドメインで作成されたオブジェクトが表示されます。このオブジェクトは編集できます。先祖ドメインで作成されたオブジェクトも表示されますが、ほとんどの場合これは編集できません。子孫ドメインにあるオブジェクトを表示および編集するには、そのドメインに切り替えます。

（注） オブジェクトがISE/ISE-PIC統合設定で使用されている場合は、オブジェクトにCRLを追加しても影響はありません。

手順

ステップ1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ2 [PKI] ノードを展開し、[信頼できるCA（Trusted CAs）] を選択します。

ステップ3 信頼できるCAオブジェクトの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ4 [CRLの追加（Add CRL）] をクリックして、DERまたはPEMでエンコードされたCRLファイルをアップロードします。

ステップ5 [OK] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

外部証明書オブジェクト

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSLルールで外部証明書オブジェクトとグループを使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。たとえば、信頼できる自己署名サーバ証明書をアップロードできますが、信頼できるCA証明書を使って検証することはできません。

X.509 v3サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書がPEM形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

外部証明書オブジェクトの追加

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）	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 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[外部証明書（External Certs）] を選択します。

ステップ 3 [外部証明書の追加（Add External Cert）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- アクティブなポリシーがオブジェクトを参照する場合は、設定の変更を展開します（設定変更の導入 を参照）。

内部証明書オブジェクト

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。内部証明書オブジェクトとグループは、以下で使用することができます。

- SSL ルール。既知の秘密キーを使用する組織のサーバの 1 つに着信するトラフィックを復号します。
- ISE/ISE-PIC 接続。[MC サーバ証明書（MC Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。
- キャプティブ ポータル設定。ユーザの Web ブラウザに接続する際にキャプティブ ポータル デバイスのアイデンティティを認証するように設定します。[サーバ証明書（Server Certificate）] フィールド用の内部証明書オブジェクトを選択します。

X.509 v3 RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることにより、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、使用中の内部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再度展開する必要があります。

内部証明書オブジェクトの追加

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）	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 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択します。

ステップ 2 [PKI] ノードを展開し、[内部証明書（Internal Certs）] を選択します。

ステップ 3 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 4 名前を入力します。

マルチドメイン展開では、オブジェクト名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないオブジェクトの名前との競合を特定することができます。

ステップ 5 [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 [キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロードする秘密キー ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 [保存（Save）] をクリックします。

証明書の登録オブジェクト

トラストポイントを使用すると、CA と証明書の管理およびトラックを行えます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

証明書の登録オブジェクトには、証明書署名要求（CSR）を作成したり、指定された CA からアイデンティティ証明書を取得したりするために必要な証明機関（CA）サーバ情報や登録パラメータが含まれています。これらのアクティビティは、秘密キー インフラストラクチャ（PKI）で発生します。

証明書の登録オブジェクトには、証明書失効情報も含まれている場合があります。PKI、デジタル証明書、および証明書の登録の詳細については、PKI インフラストラクチャとデジタル証明書 を参照してください。

証明書の登録オブジェクト の使用方法

証明書の登録オブジェクト は、管理対象デバイスを PKI インフラストラクチャに登録し、以下を実行することで VPN 接続をサポートするデバイス上にトラストポイント（CA オブジェクト）を作成するために使用されます。

1. 証明書の登録オブジェクトの CA 認証と登録のパラメータを定義します。共有パラメータを指定し、オーバーライド機能を使用して、異なるデバイスに固有のオブジェクト設定を指定します。
2. アイデンティティ証明書を必要とする各管理対象デバイスにこのオブジェクトを関連付けてインストールします。デバイス上で、そのオブジェクトはトラストポイントになります。

   証明書の登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに、証明書の登録プロセスが開始されます。プロセスは、自己署名および SCEP 登録タイプの場合は自動的に行われます。つまり、管理者による追加のアクションは必要ありません。手動による証明書の登録と PKCS12 ファイルのインポートを行うには、管理者による追加のアクションが必要です。
3. 作成されたトラストポイントを VPN の設定で指定します。

証明書の登録オブジェクトの管理

証明書の登録オブジェクトを管理するには、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] に移動し、ナビゲーション ウィンドウから [PKI] > [証明書の登録（Certificate Enrollment）] を選択します。次の情報が表示されます。

- 既存の証明書の登録オブジェクトは、[名前（Name）] 列に表示されます。

  リストをフィルタリングするには検索フィールド（虫めがね）を使用します。

- 各オブジェクトの登録タイプが [タイプ（Type）] 列に表示されます。次の登録方式を使用できます。

  - [自署（Self Signed）]：管理対象デバイスが独自の自己署名ルート証明書を生成します。
  - [SCEP]：（デフォルト）Simple Certificate Enrollment Protocol は、CA からアイデンティティ証明書を取得するためにデバイスで使用されます。
  - [手動（Manual）]：登録のプロセスは、管理者によって手動で実行されます。
  - PKCS12 ファイル（PKCS12 File）：VPN の接続をサポートする Firepower Threat Defense の管理対象デバイスで PKCS12 ファイルをインポートします。PKCS#12、つまり PFX ファイルは、サーバ証明書、中間証明書、および秘密キーを 1 つの暗号化されたファイルに保管します。

- [オーバーライド（Override）] 列は、オブジェクトがオーバーライド（緑のチェック マーク）を許可するかしないか（赤の X）を示します。数が表示される場合、これはオーバーライドの数です。

  [オーバーライド（Override）] オプションを使用して、VPN 設定の一部である各デバイスのオブジェクト設定をカスタマイズします。オーバーライドすると、各デバイスのトラストポイントの詳細が一意になります。通常、共通名またはサブジェクトは、VPN の設定内の各デバイスに対して上書きされます。

  任意のタイプのオブジェクトのオーバーライドに関する詳細および手順については、オブジェクトのオーバーライド （9 ページ） を参照してください。

- 編集アイコン（鉛筆）をクリックして、前に作成した 証明書の登録オブジェクト を**編集**します。編集は、登録オブジェクトがどの管理対象デバイスにも関連付けられていない場合にのみ実行できます。証明書の登録オブジェクトの編集については、追加の手順を参照してください。

- 削除アイコン（ごみ箱）をクリックして、前に作成した 証明書の登録オブジェクト を**削除**します。管理対象デバイスに関連付けられている証明書の登録オブジェクトは削除できません。

[（+）証明書登録の追加（(+) Add Cert Enrollment）] を押して、[証明書登録の追加（Add Cert Enrollment）] ダイアログを開き、証明書の登録オブジェクト を設定します。証明書の登録オブジェクト の追加 （83 ページ） を参照してください。次に、管理対象のヘッドエンド デバイスごとに証明書をインストールします。

関連トピック

自己署名登録を使用した証明書のインストール
SCEP の登録を使用した証明書のインストール
手動登録を使用した証明書のインストール
PKCS12 ファイルのインポートによる証明書のインストール

証明書の登録オブジェクト 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）
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	任意（Any）	Admin/Network Admin

手順

ステップ 1 以下の方法のいずれかにより、[証明書登録の追加（Add Cert Enrollment）] ダイアログを開きます。

- オブジェクト管理から直接開く：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] 画面で、[ナビゲーション（Navigation）] ペインの [PKI] > [証明書の登録（Cert Enrollment）] を選択し、[証明書の登録の追加（Add Cert Enrollment）] を押します。
- 管理対象デバイスの設定中に開く：[デバイス（Devices）] > [証明書（Certificates）] 画面で、[追加（Add）] > [新しい証明書の追加（Add New Certificate）] を選択し、[証明書の登録（Certificate Enrollment）] フィールドの **(+)** をクリックします。

ステップ 2 [名前（Name）] を入力し、任意で登録するオブジェクトの [説明（Description）] を入力します。

登録が完了すると、この名前が関連付けられた管理対象デバイスのトラストポイントの名前になります。

ステップ 3 [CA 情報（CA Information）] タブを開いてから、[登録タイプ（Enrollment Type）] を選択します。

- [自己署名証明書（Self-Signed Certificate）]：管理対象デバイスが CA として機能し、自己の署名付きルート証明書を生成します。このペインでは、さらに必要となる情報はありません。

  （注） 自己署名証明書を登録するときには、証明書パラメータで共通名（CN）を指定する必要があります。

- [SCEP]：（デフォルト）Simple Certificate Enrollment Protocol。SCEP 情報を指定します。証明書の登録オブジェクト SCEP オプション （84 ページ）を参照してください。
- [手動（Manual）]：取得した CA 証明書を [CA 証明書（CA Certificate）] フィールドに貼り付けます。CA 証明書は別のデバイスからコピーして取得できます。

- [PKCS12 ファイル（PKCS12 File）]：VPN 接続をサポートしている Firepower Threat Defense 管理対象デバイスの PKCS 12 ファイルをインポートします。PKCS#12 ファイル、または PFX ファイルは、サーバ証明書、中間証明書、秘密キーが含まれる単一の暗号化ファイルです。

ステップ 4 （任意）[証明書のパラメータ（Certificate Parameters）] タブを開き、証明書の内容を指定します。証明書の登録オブジェクト 証明書のパラメータ （85 ページ）を参照してください。

この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

ステップ 5 （任意）[キー（Key）] タブを開き、キーの内容を指定します。証明書の登録オブジェクトの主要なオプション （86 ページ）を参照してください。

ステップ 6 （任意）[失効（Revocation）] タブをクリックし、失効のオプションを指定します。証明書の登録オブジェクト 失効オプション （87 ページ） を参照してください。

ステップ 7 必要に応じ、このオブジェクトについて [オーバーライドを許可（Allow Overrides）] しておきます。オブジェクトのオーバーライドの詳細は オブジェクトのオーバーライド （9 ページ）を参照してください。

次のタスク

デバイスのトラストポイントを作成するため、デバイスの登録オブジェクトの関連付けとインストールを行います。

関連トピック

自己署名登録を使用した証明書のインストール
SCEP の登録を使用した証明書のインストール
手動登録を使用した証明書のインストール
PKCS12 ファイルのインポートによる証明書のインストール

証明書の登録オブジェクト SCEP オプション

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追加（(+) Add PKI Enrollment）] を押して、[PKI 登録の追加（Add PKI Enrollment）] ダイアログを開き、[CA 情報（CA Information）] タブを選択します。

フィールド

[登録タイプ（Enrollment Type）]：[SCEP] に設定します。

[登録 URL（Enrollment URL）]：デバイスが登録を試行する先の CA サーバの URL。

`http://CA_name:port` の形式の HTTP URL を使用します。ここで、CA_name は CA サーバのホスト DNS 名または IP アドレスです。ポート番号は必須です。

CA でのCA cgi-bin スクリプト位置がデフォルト（/cgi-bin/pkiclient.exe）でない場合は、その標準以外のスクリプト位置を http://CA_name:port/script_location の形式で URL に含める必要があります。ここで、script_location は CA スクリプトへのフル パスです。

[チャレンジ パスワード/パスワードの確認（Challenge Password/Confirm Password）]：CA サーバがデバイスのIDを検証するために使用するパスワード。CAサーバに直接アクセスして、またはWebブラウザにアドレス（**http://URLHostName/certsrv/mscep/mscep.dll**）を入力して、パスワードを取得できます。このパスワードは、CA サーバから取得した時間から60分間有効です。したがって、パスワードは、作成後、できるだけ迅速に配布する必要があります。

[再試行期間（Retry Period）]：証明書要求の試行間隔（分数）。値には1～60分を指定できます。デフォルトは1分です。

[再試行回数（Retry Count）]：最初の要求時に証明書が発行されていない場合、実行する再試行回数。1 ～ 100 の値を指定できます。デフォルトは 10 です。

[CA 証明書の取得元（CA Certificate Source）]：CA 証明書の取得方法を指定します。

- [SCEP を使用した取得（Retrieve Using SCEP）]（デフォルトであり、唯一サポートされているオプション）：Simple Certificate Enrollment Process（SCEP）を使用して CA サーバから証明書を取得します。SCEP を使用するにはデバイスと CA サーバとの間の接続が必要です。登録プロセスを開始する前に、デバイスから CA サーバへのルートがあることを確認します。

[フィンガープリント（Fingerprint）]：SCEP を使用して CA 証明書を取得する場合、CA サーバのフィンガープリントを入力する必要があります。フィンガープリントを使用してCAサーバの証明書の真正性を確認すると、不正な第三者が、本物の証明書を偽の証明書に置き換えることを阻止できます。CA サーバの [フィンガープリント（Fingerprint）] には 16 進数形式で入力します。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。サーバに直接アクセスして、または Web ブラウザにアドレス（**http://<URLHostName>/certsrv/mscep/mscep.dll**）を入力して、CAのフィンガープリントを取得します。

証明書の登録オブジェクト 証明書のパラメータ

CA サーバに送信される証明書要求に、その他の情報を指定します。この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追加（(+) Add PKI Enrollment）] を押して、[PKI 登録の追加（Add PKI Enrollment）] ダイアログを開き、[証明書のパラメータ（Certificate Parameters）] タブを選択します。

フィールド

標準の LDAP X.500 形式を使用して、すべての情報を入力します。

- [FQDN を含む（Include FQDN）]：デバイスの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を証明書要求に含めるかどうかを指定します。選択肢は次のとおりです。
  - **[デバイスのホスト名を FQDN として使用（Use Device Hostname as FQDN）]**
  - **[証明書には FQDN を使用しない（Don't use FQDN in certificate）]**
  - [カスタム FQDN（Custom FQDN）]：これを選択し、表示された [カスタム FQDN（Custom FQDN）] フィールドに指定します。
- [デバイスの IP アドレスを含める（Include Device's IP Address）]：IP アドレスが証明書要求に含まれているインターフェイス。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。

（注） 自己署名証明書を登録するときには、証明書パラメータで共通名（CN）を指定する必要があります。

- [組織単位（OU）（Organizational Unit (OU)）]：証明書に含める組織単位の名前（部門名など）。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [地域（L）（Locality (L)）]：証明書に含める地域。
- [都道府県（ST）（State (ST)）]：証明書に含める州または都道府県。
- [国コード（C）（County Code (C)）]：証明書に含める国。これらのコードは、ISO 3166 の国の省略形に準拠しています（たとえばアメリカ合衆国は「US」）。
- [電子メール（E）（Email (E)）]：証明書に含める電子メール アドレス。
- [デバイスのシリアル番号を含める（Include Device's Serial Number）]：デバイスのシリアル番号を証明書に含めるかどうかを指定します。CA は、このシリアル番号を使用して、証明書を認証するか、またはあとで証明書を特定のデバイスに関連付けます。シリアル番号を含めるかどうか判断できない場合は、デバッグに役立つため、含めてください。

証明書の登録オブジェクト の主要なオプション

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追加（(+) Add PKI Enrollment）] を押して、[PKI 登録の追加（Add PKI Enrollment）] ダイアログを開き、[キー（Key）] タブを選択します。

フィールド

- [キー タイプ（Key Type）]：RSA（デフォルト、およびサポートされるオプションのみ）または ECDSA。
- [キー名（Key Name）]：証明書と関連付けるキー ペアが既に存在する場合、このフィールドではそのキー ペアの名前を指定します。キー ペアが存在しない場合、このフィールドには登録中に生成されるキー ペアに指定する名前を指定します。RSA キー ペアを指定しない場合、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が代わりに使用されます。
- [キー サイズ（Key Size）]：キー ペアが存在しない場合は、必要なキー サイズ（係数）をビットで定義します。推奨サイズは 1024 です。係数のサイズが大きくなるほど、キーがよりセキュアになります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり（512 ビットより大きい場合は 1 分以上）、交換するときの処理にも時間がかかります。

証明書の登録オブジェクト 失効オプション

証明書の失効ステータスを確認するかどうかを、方法を選択して設定することで指定します。失効の確認はデフォルトでオフになっており、どちらの方法（CRL または OCSP）もオンになっていません。

Firepower Management Center ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] の次に、ナビゲーション ウィンドウから **[PKI] > [PKI 登録（PKI Enrollment）]** を選択します。[（+）PKI 登録の追加（(+) Add PKI Enrollment）] を押して、[PKI 登録の追加（Add PKI Enrollment）] ダイアログを開き、[失効（Revocation）] タブを選択します。

フィールド

- [証明書失効リストの有効化（Enable Certificate Revocation Lists）]：CRL の確認を有効にするにはオンにします。
  - [証明書からの CRL 分散ポイント（Use CRL distribution point from the certificate）]：証明書からの失効リスト配布 URL を取得するにはオンにします。
  - [設定された静的 URL を使用（Use static URL configured）]：失効リストのスタティックな事前定義された配布 URL を追加するには、これをオンにします。次に URL を追加します。

    [CRL サーバの URL（CRL Server URLs）]：CRL をダウンロード可能な LDAP サーバの URL。この URL は **`ldap://`** から始まり、URL にはポート番号が含まれる必要があります。

- [Online Certificate Status Protocol（OCSP）の有効化（Enable Online Certificate Status Protocol）]：OCSP チェックを有効にするにはオンにします。

  [OCSP サーバ URL（OCSP Server URL）]：OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**`http://`** で始まる必要があります。

- [失効情報にアクセスできない場合、証明書は有効と見なされます（Consider the certificate valid if revocation information can not be reached）]：デフォルトでオンになっています。これを許可しない場合は、チェックボックスをオフにします。

SLA モニタ オブジェクト

各 SLA モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。要求がタイムアウトすると、そのルートはルーティング テーブルから削除され、バックアップ ルートに置き換えられます。SLA モニタリング ジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージング アウトしません）。SLA モニタ オブジェクトは、IPv4 スタティック ルート ポリシーの [ルート トラッキング（Route Tracking）] フィールドで使用されます。IPv6 ルートでは、ルート トラッキングによって SLA モニタを使用することはできません

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから [SLA モニタ（SLA Monitor）] を選択します。

ステップ 2 [SLA モニタの追加（Add SLA Monitor）] をクリックします。

ステップ 3 [名前（Name）] フィールドにオブジェクトの名前を入力します。

ステップ 4 （オプション）[説明（Description）] フィールドにオブジェクトの説明を入力します。

ステップ 5 [頻度（Frequency）] フィールドに、ICMP エコー要求送信の頻度（秒単位）を入力します。有効な値の範囲は、1 ～ 604800 秒（7 日）です。デフォルトは 60 秒です。

（注） 頻度はタイムアウト値未満にできません。これらの値を比較するには、頻度をミリ秒に換算する必要があります。

ステップ 6 [SLA モニタ ID（SLA Monitor ID）] フィールドに SLA 操作の ID 番号を入力します。値の範囲は 1 ～ 2147483647 です。1 つのデバイスには最大で 2000 個の SLA 操作を作成できます。各 ID 番号はポリシーとデバイス設定に対して一意である必要があります。

ステップ 7 [しきい値（Threshold）] フィールドに、上昇しきい値が宣言されるまでに、ICMP エコー要求の後に経過する必要のある時間（ミリ秒単位）を入力します。有効な値の範囲は、0 ～ 2147483647 ミリ秒です。デフォルトは 5000 ミリ秒です。しきい値は、定義された値を超過したイベントを示すためだけに使用されます。これらのイベントは、タイムアウト値が適切であ

るかどうかを評価するために使用できます。このイベントは、モニタリング対象のアドレスへの到達可能性を直接的に示すものではありません。

（注） しきい値はタイムアウト値を超過しないようにします。

ステップ 8 [タイムアウト（Timeout）] フィールドに、SLA 操作が ICMP エコー要求への応答を待機する時間（ミリ秒単位）を入力します。値の範囲は 0 ～ 604800000 ミリ秒（7 日）です。デフォルトは 5000 ミリ秒です。モニタリング対象のアドレスからの応答がこのフィールドに定義された時間内に受信されない場合、スタティック ルートがルーティング テーブルから削除され、バックアップ ルートに置き換えられます。

（注） タイムアウト値は頻度値を超過できません。2 つの数値を比較するには、頻度値をミリ秒に換算してください。

ステップ 9 [データ サイズ（Data Size）] フィールドに、ICMP 要求パケット ペイロードのサイズ（バイト単位）を入力します。値の範囲は 0 ～ 16384 バイトです。デフォルトは 28 バイトです。この場合、全体の ICMP パケットは 64 バイトとなります。この値には、プロトコルまたは Path Maximum Transmission Unit（PMTU）で許可される最大値を超える値を設定しないでください。場合によっては、到達可能性を確保するために、デフォルトのデータ サイズを大きくして、ソースとターゲットの間での PMTU の違いを検出できるようにすることが必要となります。PMTU が小さいと、セッションのパフォーマンスに影響を及ぼすことがあります。セッションのパフォーマンスへの影響が検出されると、セカンダリ パスが使用されます。

ステップ 10 [ToS] フィールドに、ICMP 要求パケットの IP ヘッダーで定義されたタイプ オブ サービス（ToS）の値を入力します。値の範囲は 0 ～ 255 です。デフォルトは 0 です。このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。この情報は、ポリシー ルーティングのためにネットワーク上の他のデバイスが使用する場合もあれば、専用アクセス レートなどの機能によって使用される場合もあります。

ステップ 11 [パケット数（Number of Packets）] フィールドに、送信されるパケットの数を入力します。値の範囲は 1 ～ 100 です。デフォルトは 1 パケットです。

（注） パケット損失によって、Firepower Threat Defense デバイスがモニタリング対象のアドレスに到達できないと誤って認識することが懸念される場合は、デフォルトのパケット数を大きくしてください。

ステップ 12 [モニタリング対象アドレス（Monitored Address）] フィールドに、SLA 操作によって可用性がモニタされている IP アドレスを入力します。

ステップ 13 [ゾーン/インターフェイス（Zones/Interfaces）] リストで、デバイスが管理ステーションと通信するインターフェイスを含むゾーンを追加します。ゾーン内にないインターフェイスの場合は、[選択したゾーン/インターフェイス（Selected Zone/Interface）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

ステップ 14 [保存（Save）] をクリックします。

プレフィックス リスト

ルート マップ、ポリシー マップ、OSPF フィルタリング、BGP ネイバー フィルタリングを設定する際に使用する、IPv4 および IPv6 用のプレフィックス リスト オブジェクトを作成できます。

IPv6 プレフィックス リストの設定

IPv6 プレフィックス リストの設定ページを使用して、プレフィックス リスト オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、目次で **[プレフィックス リスト（Prefix Lists）] > [IPv6 プレフィックス リスト（IPv6 Prefix List）]** を選択します。

ステップ 2 [プレフィックス リストの追加（Add Prefix List）] をクリックします。

ステップ 3 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウの [名前（Name）] フィールドで、プレフィックス リスト オブジェクトの名前を入力します。

ステップ 4 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 5 [アクション（Action）] ドロップダウンリストから適切なアクション、[許可（Allow）] または [ブロック（Block）] を選択して、再配布アクセスを指定します。

ステップ 6 このオブジェクトですでに設定されているプレフィックスリストエントリのリストにおける、新しいプレフィックスリストエントリの位置を示す固有の数字を、[シーケンス番号（Sequence No.）] フィールドに入力します。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。

ステップ 7 [IP アドレス（IP address）] フィールドの IP アドレス/マスク長形式で、IPv6 アドレスを指定します。マスク長は 1 ～ 128 の有効な値でなければなりません。

ステップ 8 [最小プレフィックス長（Minimum Prefix Length）] フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。

ステップ 9 [最大プレフィックス長（Maximum Prefix Length）] フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 12 [保存（Save）] をクリックします。

IPv4 プレフィックス リストの設定

IPv4 プレフィックス リストの設定ページを使用して、プレフィックス リスト オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、OSPF フィルタリングまたは BGP ネイバー フィルタリングを設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択し、目次で [プレフィックス リスト（Prefix Lists）] > [IPv4 プレフィックス リスト（IPv4 Prefix List）] を選択します。 > >

ステップ 2 [プレフィックス リストの追加（Add Prefix List）] をクリックします。

ステップ 3 [新しいプレフィックス リスト オブジェクト（New Prefix List Object）] ウィンドウの [名前（Name）] フィールドで、プレフィックス リスト オブジェクトの名前を入力します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [アクション（Action）] ドロップダウンリストから適切なアクション、[許可（Allow）] または [ブロック（Block）] を選択して、再配布アクセスを指定します。

ステップ 6 このオブジェクトですでに設定されているプレフィックス リストエントリのリストにおける、新しいプレフィックス リストエントリの位置を示す固有の数字を、[シーケンス番号（Sequence No.）] フィールドに入力します。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。

ステップ 7 [IP アドレス（IP address）] フィールドの IP アドレス/マスク長形式で、IPv4 アドレスを指定します。マスク長は 1 ～ 32 の有効な値でなければなりません。

ステップ 8 [最小プレフィックス長（Minimum Prefix Length）] フィールドで最小プレフィックス長を入力します。値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。

ステップ 9 [最大プレフィックス長（Maximum Prefix Length）] フィールドで最大プレフィックス長を入力します。値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

ステップ 10 [追加（Add）] をクリックします。

ステップ 11 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 12 [保存（Save）] をクリックします。

ルート マップ

ルート マップは、ルートをルーティング プロセスに再配布するときに使用できます。また、デフォルト ルートをルーティング プロセスに生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。ルート マップを設定して、ルート マップ オブジェクトの新しいルート マップ エントリを作成したり、既存のルート マップ エントリを編集したりします。

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

始める前に

ルート マップは、これらのオブジェクトの 1 つまたは複数を使用することができます。これらのオブジェクトをすべて追加する必要はありません。これらのオブジェクトを必要に応じて作成および使用して、ルート マップを設定します。

- ACL の追加
- プレフィックス リストの追加
- AS パスの追加
- コミュニティ リストの追加
- ポリシー リストの追加

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[ルート マップ（Route Map）]** を選択します。

ステップ 2 [ルート マップの追加（Add Route Map）] をクリックします。

ステップ 3 [新しいルート マップ オブジェクト（New Route Map Object）] ウィンドウで [追加（Add）] をクリックします。

ステップ 4 [シーケンス番号（Sequence No.）] フィールドで、このルート マップ オブジェクトにすでに設定されているルート マップ エントリのリストでの新しいルート マップ エントリの位置を示す、0 ～ 65535 の番号を入力します。

（注） 将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、少なくとも 10 単位で句に番号を指定することをお勧めします。

ステップ 5 [再配布（Redistribution）] ドロップダウン リストから、再配布アクセスを示す適切なアクション（[許可（Allow）] または [ブロック（Block）]）を選択します。

ステップ 6 [句の照合（Match Clauses）] タブをクリックして、コンテンツ テーブルで選択する次の条件に基づいて照合します（ルート/トラフィック）。

- [セキュリティ ゾーン（Security Zones）]：（I/O）インターフェイスに基づいてトラフィックを照合します。ゾーンを選択して追加するか、インターフェイス名を入力して追加します。
- [IPv4]：次の条件に基づいて IPv4（ルート/トラフィック）を照合します。条件を定義するタブを選択します。
  1. ルート アドレスに基づいてルートを照合するには、[アドレス（Address）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
  2. ルートのネクスト ホップ アドレスに基づいてルートを照合するには、[ネクスト ホップ（Next Hop）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
  3. ルートのアドバタイズ送信元アドレスに基づいてルートを照合するには、[ルート送信元（Route Source）] タブをクリックします。IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。
- [IPv6]：ルート：ルートのルート アドレス、ネクストホップ アドレス、またはアドバタイズ送信元アドレスに基づいて IPv6（ルート/トラフィック）を照合します。

- [BGP]：次の条件に基づいてBGP（ルート/トラフィック）を照合します。条件を定義するタブを選択します。

  1. BGP 自律システム パス アクセス リストと指定されたパス アクセス リストの照合を有効にするには、[AS パス（AS Path）] タブをクリックします。複数のパス アクセス リストを指定した場合、ルートはいずれかのパス アクセス リストと一致します。
  2. BGP コミュニティと指定されたコミュニティの照合を有効にするには、[コミュニティ リスト（Community List）] タブをクリックします。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンド ルート マップにアドバタイズされません。
  3. BGP ポリシーを評価および処理するためのルート マップを設定するには、[ポリシー リスト（Policy List）] タブをクリックします。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

- [その他（Others）]：次の条件に基づいてルートまたはトラフィックを照合します。

  1. ルートのメトリックの照合を有効にするには、[メトリック ルート値（Metric Route Value）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。
  2. [タグ値（Tag Values）] フィールドに、照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。
  3. ルート タイプの照合を有効にするには、適切な**ルート タイプ** オプションをオンにします。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。複数のルート タイプをリストから選択することができます。

ステップ 7 [句の設定（Set Clauses）] タブをクリックして、コンテンツ テーブルで選択する次の条件に基づいてルート/トラフィックを設定します。

- [メトリック値（Metric Values）]：[帯域幅（Bandwidth）]、すべての値、または値なしを設定します。

  1. [帯域幅（Bandwidth）] フィールドに、メトリック値または帯域幅（キロビット/秒）を入力します。有効な値は、0 ～ 4294967295 の範囲の整数値です。
  2. [メトリック タイプ（Metric Type）] ドロップダウン リストから、宛先ルーティング プロトコルのメトリックのタイプを選択して指定します。有効な値は、internal、type-1、または type-2 です。
  3. [遅延（Delay）] フィールドに、EIGRP ルートの遅延を 10 マイクロ秒単位で入力します。有効な値の範囲は、1 ～ 4294967295 です。

4. [信頼性（Reliability）] フィールドに、EIGRP のパケット伝送の成功率を入力します。有効な値の範囲は 0 ～ 255 です。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
5. [有効（Effective）] フィールドに、EIGRP の有効な帯域幅を入力します。有効な値の範囲は 1 ～ 255 です。値 255 は、100% のロードを意味します。
6. [MTU] フィールドに、EIGRP のルートの最小 MTU サイズをバイト単位で入力します。有効な値の範囲は 1 ～ 4294967295 です。

- [BGP 句（BGP Clauses）] : 次の条件に基づいて BGP ルートを設定します。条件を定義するタブを選択します。

1. BGP ルートの自律システム パスを変更するには、[AS パス（AS Path）] タブをクリックします。
    1. 任意の自律システム パス文字列を BGP ルートの前に付加するには、[AS パスを前に付加（Prepend AS Path）] タブをクリックします。通常、ローカルな AS 番号が複数回追加され、自律システム パス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。
    2. 最後の AS 番号を AS パスの前に付加するには、[最後の AS を AS パスの前に付加（Prepend Last AS to AS Path）] フィールドに AS パス番号を入力します。AS 番号の値を 1 ～ 10 の範囲で入力します。
    3. ルートのタグを自律システム パスに変換するには、[ルート タグを AS パスに変換する（Convert route tag into AS path）] チェックボックスをオンにします。
2. コミュニティ属性を設定するには、[コミュニティ リスト（Community List）] タブをクリックします。
    1. ルート マップをパスするプレフィックスからコミュニティ属性を除去するには、[なし（None）] ラジオ ボタンをクリックします。
    2. コミュニティ番号を入力するには、[コミュニティの指定（Specify Community）] ラジオ ボタンをクリックします（必要な場合）。有効な値は 1 ～ 4294967295 です。
    3. 既存のコミュニティにコミュニティを追加するには、[既存のコミュニティに追加する（Add to existing communities）] チェックボックスをオンにします。
    4. 既知のコミュニティのいずれかを使用するには、[インターネット（Internet）]、[アドバタイズなし（No-Advertise）]、または [エクスポートなし（No-Export）] チェックボックスをオンにします。
3. 追加属性を設定するには、[その他（Others）] タブをクリックします。
    1. タグ値を自動的に計算するには、[自動タグを設定する（Set Automatic Tag）] チェックボックスをオンにします。

2. [ローカル優先度の設定（Set Local Preference）] フィールドに自律システム パスの優先度値を入力します。0 から 4294967295 までの値を入力してください。
3. [重み付けの設定（Set Weight）] フィールドにルーティング テーブルの BGP ウェイトを入力します。0 から 65535 までの値を入力してください。
4. BGP の発信元コードを選択して指定します。有効な値は [ローカル IGP（Local IGP）] および [未完了（Incomplete）] です。
5. [IPv4 設定（IPv4 Settings）] セクションで、パケットが出力されるネクスト ホップのネクスト ホップ IPv4 アドレスを指定します。隣接ルータである必要はありません。複数の IPv4 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。

   [プレフィックス リスト（Prefix List）] ドロップダウン リストから IPv4 プレフィックス リストを選択して指定します。
6. [IPv6 設定（IPv4 Settings）] セクションで、パケットが出力されるネクスト ホップのネクスト ホップ IPv6 アドレスを指定します。隣接ルータである必要はありません。複数の IPv6 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。

   [プレフィックス リスト（Prefix List）] ドロップダウン リストから IPv6 プレフィックスを選択して指定します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 10 [保存（Save）] をクリックします。

アクセス リスト

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

アクセス リスト オブジェクトは、アクセス コントロール リスト（ACL）とも呼ばれ、トラフィックに適用されるサービスを選択します。アクセス リスト オブジェクトを使って、ルート マップなどの機能を設定します。ACL で許可されたトラフィックはサービスを利用できま

すが、「ブロックされた」トラフィックはサービスから除外されます。サービスから除外されたトラフィックが必ずしも完全にドロップされるわけではありません。

次のタイプの ACL を設定できます。

- 拡張：送信元と宛先アドレスおよびポートに基づいてトラフィックを識別します。IPv4 および IPv6 アドレスをサポートしており、任意のルールで混在させることができます。
- 標準：宛先アドレスのみに基づいてトラフィックを識別します。IPv4 のみサポートしています。

ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）またはルールで構成されます。ACE の順番は重要です。パケットを「許可」 ACE と照合して ACL を評価する際、ACL に登録されている ACE の順番どおりに照合します。一致が見つかると、それ以降の ACE とは照合しません。たとえば、10.100.10.1 を「許可」して、10.100.10.0/24 の残りはすべて「ブロック」する場合、許可エントリがブロック エントリより前に登録されている必要があります。通常、具体性の高いルールを ACL の上部に置きます。

「許可」エントリに一致しないパケットはブロックされたと見なします。

次に、ACL オブジェクトの設定方法について説明します。

拡張 ACL オブジェクトの設定

送信元および宛先アドレス、プロトコル、およびポートに基づいて、あるいはトラフィックが IPv6 の場合にトラフィックを照合するには、拡張 ACL オブジェクトを使用します。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[アクセス コントロール リスト（Access Control Lists）]** > **[拡張（Extended）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [拡張 ACL の追加（Add Extended ACL）] をクリックして、新しいオブジェクトを作成します。
- 編集アイコン（）をクリックして、既存のオブジェクトを編集します。

ステップ 3 [拡張 ACL オブジェクト（Extended ACL Object）] ダイアログボックスで、オブジェクトの名前を入力し（スペースは使用不可）、アクセス コントロール エントリを設定します。

a) 次のいずれかを実行します。

- [追加（Add）] をクリックして、新しいエントリを作成します。
- 編集アイコン（）をクリックして、既存のエントリを編集します。

右クリック メニューからも、エントリの切り取り、コピー、貼り付け、または削除を行うことができます。

b) トラフィック基準を許可（一致）するか、またはブロック（一致しない）するかの**アクション**を選択します。

（注） [ログ（Logging）]、[ログ レベル（Log Level）]、および[ログ インターバル（Log Interval）] オプションはアクセス ルールに対してのみ使用されます（インターフェイスに接続されているか、グローバルで適用される ACL）。ACL オブジェクトがアクセス ルールで使用されていないため、これらの値にはデフォルトを使用します。

c) 次のテクニックのいずれかを使用して、[ネットワーク（Network）] タブで送信元および宛先アドレスを設定します。

- [利用可能（Available）] リストから目的のネットワーク オブジェクトまたはグループを選択し、[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。リストの上の [+] ボタンをクリックすると、新しいオブジェクトを作成できます。IPv4 アドレスと IPv6 アドレスを組み合わせることができます。
- 送信元または宛先リストの下の編集ボックスにアドレスを入力し、[追加（Add）] をクリックします。1 つのホスト アドレス（10.100.10.5、2001:DB8::0DB8:800:200C:417A など）またはサブネット（10.100.10.0/24 または 10.100.10.0 255.255.255.0 の形式。IPv6 の場合は 2001:DB8:0:CD30::/60）を指定できます。

d) [ポート（Port）] タブをクリックし、次のテクニックのいずれかを使用してサービスを設定します。

- [利用可能（Available）] リストから目的のポート オブジェクトまたはグループを選択し、[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。リストの上の [+] ボタンをクリックすると、新しいオブジェクトを作成できます。オブジェクトによって TCP/UDP ポート、ICMP/ICMPv6 メッセージ タイプ、その他のプロトコルを指定できます（「任意」を含む）。ただし、通常は空にしておく送信元ポートは TCP/UDP のみを受け入れます。
- 送信元または宛先リストの下の編集ボックスでポートまたはプロトコルを入力または選択し、[追加（Add）] をクリックします。

（注） すべての IP トラフィックに適用するエントリを取得するには、「すべて」のプロトコルを指定する宛先ポート オブジェクトを選択します。

e) [追加（Add）] をクリックして、エントリをオブジェクトに追加します。
f) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

ステップ 4 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 5 [保存（Save）] をクリックします。

標準 ACL オブジェクトの設定

宛先 IPv4 アドレスのみに基づいてトラフィックを照合する場合は、標準 ACL オブジェクトを使用します。それ以外の場合は、拡張 ACL を使用します。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから **[アクセス コントロール リスト（Access Control Lists）] > [標準（Standard）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [標準 ACL の追加（Add Standard ACL）] をクリックして、新しいオブジェクトを作成します。
- 編集アイコン（  ）をクリックして、既存のオブジェクトを編集します。

ステップ 3 [標準 ACL オブジェクト（Standard ACL Object）] ダイアログボックスで、オブジェクトの名前を入力し（スペースは使用できません）、アクセス コントロール エントリを設定します。

a) 次のいずれかを実行します。

- [追加（Add）] をクリックして、新しいエントリを作成します。
- 編集アイコン（  ）をクリックして、既存のエントリを編集します。

右クリック メニューからも、エントリの切り取り、コピー、貼り付け、または削除を行うことができます。

b) アクセス コントロール エントリごとに、次のプロパティを設定します。

- [アクション（Action）] : トラフィック基準を許可（一致）またはブロック（不一致）するかどうか。
- [ネットワーク（Network）] : IPv4 ネットワーク オブジェクトまたはトラフィックの宛先を特定するグループを追加します。

c) [追加（Add）] をクリックして、エントリをオブジェクトに追加します。

d) 必要に応じて、エントリをクリックおよびドラッグして、ルール順序で目的の場所まで上下に移動します。

このプロセスを繰り返して、オブジェクトに追加エントリを作成または編集します。

ステップ 4 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 5 [保存（Save）] をクリックします。

AS パスのオブジェクト

AS パスは BGP のセットアップの必須属性です。これは、ネットワークのアクセスを可能にする AS 番号のシーケンスです。AS パスは、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。異なる AS プレフィックスにリーチする方法に関するメッセージを交換、更新するのに、ネイバー自律システム（ASes）で BGP が使用されます。各ルータで宛先までの最適ルートに関する新たなローカル判断が行われた後、用意されている距離メトリックおよびパス属性とともに、ルートまたはパスの情報がそれぞれのピアに送信されます。この情報がネットワークを移動すると、パスに沿った各ルータは、固有の AS 番号を BGP メッセージの ASes リストの前に付加します。このリストは、ルートの AS パスです。AS パスは AS プレフィックスとともに、ネットワークを介した一方向の中継ルートの特定のハンドルになります。AS パス ページの設定を使用して、自律システム（AS）のパスのポリシー オブジェクトを作成、コピー、編集します。ルート マップ、ポリシー マップ、または BGP ネイバー フィルタリングを設定するときに使用する、AS パス オブジェクトを作成できます。AS パスのフィルタにより、正規表現でルーティング アップデート メッセージをフィルタ処理できます。

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

手順

ステップ 1 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択して、目次で [AS パス（AS Path）] を選択します。 >

ステップ 2 [AS パスの追加（Add AS Path）] をクリックします。

ステップ 3 [名前（Name）] フィールドに AS パス オブジェクトの名前を入力します。有効な値は、1 ～ 500 です。

ステップ 4 [新しい AS パス オブジェクト（New AS Path Object）] ウィンドウで、[追加（Add）] をクリックします。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。
b) [正規表現（Regular Expression）] フィールドで AS パスのフィルタ処理を定義する正規表現を指定します。
c) [追加（Add）] をクリックします。

ステップ 5 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 6 [保存（Save）] をクリックします。

コミュニティ リスト

コミュニティは、遷移的 BGP 属性のオプションです。コミュニティは、共通するいくつかの属性を共有する宛先のグループです。これはルート タギングに使用されます。BGP のコミュニティ属性は、特定のプレフィックスに割り当てられ、他のネイバーにアドバタイズされる数値です。コミュニティは、一般的な属性を共有する一連のプレフィックスのマーキングに使用できます。アップストリームプロバイダーは、これらのマーカーを使用して、特定のローカル設定のフィルタリングまたは割り当て、あるいは他の属性の変更などの一般的なルーティング ポリシーを適用します。コミュニティ リストの設定ページを使用して、コミュニティ リスト ポリシー オブジェクトを作成、コピー、編集します。ルート マップまたはポリシー マップを設定するときに使用する、コミュニティ リスト ポリシー オブジェクトを作成できます。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。コミュニティ リストは、一致ステートメントの番号付きリストです。接続先は、一致が見つかるまでルールに反する一致をします。

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

手順

ステップ 1 [オブジェクト（Objects）]>[オブジェクト管理（Object Management）] を選択して、目次で [コミュニティ リスト（Community List）] を選択します。 >

ステップ 2 [コミュニティ リストの追加（Add Community List）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、コミュニティ リスト オブジェクトの名前を指定します。

ステップ 4 [新しいコミュニティ リスト オブジェクト（New Community List Object）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 5 [標準（Standard）] オプション ボタンを選択して、コミュニティ ルールの種類を表示します。

標準コミュニティ リストは、ウェルノウン コミュニティやコミュニティ番号の指定に使用されます。

（注） 標準を使用したエントリ、コミュニティ ルールの拡張種類を使用したエントリを、同じコミュニティ リスト オブジェクトに含めることはできません。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [コミュニティ（Communities）] フィールドで、コミュニティ番号を指定します。有効な値は 1 ～ 4294967295 または 0:1 ～ 65534:65535 です。

c) 適切な [ルート タイプ（Route Type）] を選択します。

- [インターネット（Internet）]：インターネットのウェルノウン コミュニティを指定するために選択します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
- [非アドバタイズ（No Advertise）]：非アドバタイズのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。
- [非エクスポート（No Export）]：非エクスポートのウェルノウン コミュニティを指定するために選択します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 6 [拡張（Expanded）] オプション ボタンを選択して、コミュニティ ルールの種類を表示します。

拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ属性の照合パターンの指定に使用されます。

a) [アクション（Action）] ドロップダウンリストから [許可（Allow）] または [ブロック（Block）] オプションを選択して、再配布アクセスを指定します。

b) [表現（Expressions）] フィールドで、正規表現を指定します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 9 [保存（Save）] をクリックします。

ポリシー リスト

ポリシー リストのポリシー オブジェクトを作成、コピー、編集するには、[ポリシー リストの設定（Configure Policy List）] ページを使用します。ルート マップを設定するときに使用するポリシー リスト オブジェクトを作成できます。ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに

2 つ以上のポリシー リストを設定できます。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツ テーブルから [ポリシー リスト（Policy List）] を選択します。

ステップ 2 [ポリシー リストの追加（Add Policy List）] をクリックします。

ステップ 3 [名前（Name）] フィールドにポリシー リスト オブジェクトの名前を入力します。オブジェクト名では、大文字と小文字が区別されません。

ステップ 4 [アクション（Action）] ドロップダウン リストから、一致する条件へのアクセスを許可するかブロックするかを選択します。

ステップ 5 [インターフェイス（Interface）] タブをクリックして、指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。

[ゾーン/インターフェイス（Zones/Interfaces）] リストで、デバイスが管理ステーションと通信するインターフェイスを含むゾーンを追加します。ゾーン内にないインターフェイスの場合は、[選択したゾーン/インターフェイス（Selected Zone/Interface）] リストの下のフィールドにインターフェイス名を入力し、[追加（Add）]をクリックします。デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ、デバイスでホストが設定されます。

ステップ 6 [アドレス（Address）] タブをクリックして、標準アクセス リストまたはプレフィックス リストで許可された宛先アドレスを持つルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 7 [ネクスト ホップ（Next Hop）] タブをクリックして、指定したアクセス リストまたはプレフィックス リストの 1 つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 8 [ルート送信元（Route Source）] タブをクリックして、アクセス リストまたはプレフィックス リストで指定されたアドレスのルータおよびアクセス サーバによってアドバタイズされたルートを再配布します。

照合に [アクセス リスト（Access List）] または [プレフィックス リスト（Prefix List）] のどちらを使用するかを選択し、照合に使用する標準アクセス リスト オブジェクトまたはプレフィックス リスト オブジェクトを入力するか選択します。

ステップ 9 [AS パス（AS Path）] タブをクリックして、BGP 自律システム パスを一致させます。複数の AS パスを指定した場合、ルートはいずれかの AS パスと一致します。

ステップ 10 [コミュニティ ルール（Community Rule）] タブをクリックすると、BGP コミュニティと指定されたコミュニティの照合が有効になります。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。BGP コミュニティと指定したコミュニティの完全一致を有効にするには、[指定したコミュニティと完全に一致（Match the specified community exactly）] チェックボックスをオンにします。

ステップ 11 [メトリックとタグ（Metric & tag）] タブをクリックして、メトリックとルートのセキュリティ グループ タグを照合します。

a) [Metric（メトリック）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

b) [タグ（Tag）] フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティ グループ タグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。

ステップ 12 このオブジェクトのオーバーライドを許可する場合は、[オーバーライドを許可（Allow Overrides）] チェックボックスをオンにします（オブジェクトのオーバーライドの許可 （11 ページ） を参照）。

ステップ 13 [保存（Save）] をクリックします。

VPN オブジェクト

Firepower Threat Defense IKE ポリシー

Internet Key Exchange（IKE; インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）

IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKEv1 では、IKE プロポーザルには、単一のアルゴリズム セットと係数グループが含まれています。複数のポリシーをプライオリティ付きで作成して、少なくとも 1 つのポリシーがリモート ピアのポリシーに一致するようにできます。IKEv1 とは異なり、IKEv2 プロポーザルでは、1 つのポリシーで複数のアルゴリズムとモジュラス グループを選択できます。フェーズ 1 のネゴシエーションでピアを選択するため、作成する IKE プロポーザルの数を 1 つにすることは可能ですが、複数の異なる IKE プロポーザルを作成して、最も望ましいオプションを高い優先順位に設定することも検討してください。IKEv2 では、ポリシー オブジェクトは認証の指定は行わず、他のポリシーで認証の要件を定義する必要があります。

サイト間 IPsec VPN を設定する際は、IKE ポリシーが必要です。詳細については、Firepower Threat Defense の VPN を参照してください。

IKEv1 ポリシー オブジェクトの設定

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）
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

IKEv1 ポリシー ページを使用して、IKEv1 ポリシー オブジェクトを作成、削除、または編集します。これらのポリシー オブジェクトには、IKEv1 ポリシーに必要なパラメータが含まれています。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv1 ポリシー（IKEv1 Policy）]** を選択します。

前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセス レベルによっては、プロポーザルを編集（）、表示（）、または削除（）することもできます。

ステップ 2 （任意） [IKEv1 ポリシーの追加（Add IKEv1 Policy）] を選択して、新しいポリシー オブジェクトを作成します。

ステップ 3 このポリシーの [名前（Name）] を入力します。最大 128 文字を使用できます。

ステップ 4 （任意） このプロポーザルの [説明（Description）] を入力します。最大 1,024 文字を使用できます。

ステップ 5 IKE ポリシーの [プライオリティ（Priority）] 値を入力します。

このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポー

トしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。有効な値の範囲は1～65,535です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は1から始まり、次は5となり、その後は5ずつ増加します。

ステップ6 [暗号化（Encryption）] 方法を選択します。

IKEv1 ポリシーで使用する暗号化およびハッシュ アルゴリズムを決定する場合、ピア デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。IKEv1では、いずれかのオプションを選択します。オプションの説明の詳細については、使用する暗号化アルゴリズムの決定を参照してください。

ステップ7 [ハッシュ（Hash）] アルゴリズムを選択して、メッセージの整合性の確保に使用されるメッセージ ダイジェストを作成します。

IKEv1プロポーザルで使用する暗号化およびハッシュアルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。オプションの説明の詳細については、使用するハッシュアルゴリズムの決定を参照してください。

ステップ8 **[Diffie-hellman グループ（Diffie-Hellman Group）]** を設定します。

暗号化に使用するDiffie-Hellmanグループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2つのピアに、一致する係数グループが設定されている必要があります。VPNで許可するグループを選択します。オプションの説明の詳細については、使用するDiffie-Hellman 係数グループの決定を参照してください。

ステップ9 セキュリティ アソシエーション（SA）の [ライフタイム（Lifetime）]（秒数）を設定します。120 ～ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。

このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKEネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後のIPsecセキュリティアソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

ステップ10 2 つのピア間で使用する [認証方法（Authentication Method）] を設定します。

- [事前共有キー（Preshared Key）]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中にIKEで使用したりできます。参加ピアの1つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
- [証明書（Certificate）]：VPN接続に認証方式として証明書を使用すると、ピアはPKIインフラストラクチャの CA サーバからデジタル証明書を取得して、互いの認証で交換します。

（注） IKEv1 をサポートする VPN トポロジでは、選択した IKEv1 ポリシー オブジェクトで指定した [認証方式（Authentication Method）] が、IKEv1 の [認証タイプ（Authentication Type）] 設定のデフォルトになります。これらの値は一致する必要があります。一致しないと設定がエラーになります。

ステップ 11 [Save] をクリックします。
新しい IKEv1 ポリシーがリストに追加されます。

IKEv2 ポリシー オブジェクトの設定

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）
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

IKEv2 ポリシー ダイアログボックスを使用して、IKEv2 ポリシーオブジェクトを作成、削除、編集します。これらのポリシー オブジェクトには、IKEv2 ポリシーに必要なパラメータが含まれています。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv2 ポリシー（IKEv2 Policy）]** を選択します。

前に設定したポリシーは、システムによって定義されるデフォルトにリストされています。アクセス レベルによっては、ポリシーを編集（）、表示（）、または削除（）することもできます。

ステップ 2 [IKEv2 ポリシーの追加（Add IKEv2 Policy）] を選択して、新しいポリシーを作成します。

ステップ 3 このポリシーの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このポリシーの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [プライオリティ（Priority）] を入力します。

IKEプロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティ ポリシーで定義されているパラメータの使用を試行します。有効な値の範囲は 1 ～ 65535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、

管理センターによって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。

ステップ 6 セキュリティ アソシエーション（SA）の [ライフタイム（Lifetime）]（秒数）を設定します。120 ～ 2,147,483,647 秒の値を指定できます。デフォルトは 86400 です。

このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

ステップ 7 IKE ポリシーで使用するハッシュ アルゴリズムの [整合性アルゴリズム（Integrity Algorithms）] 部分を選択します。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。

IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。オプションの説明の詳細については、使用するハッシュ アルゴリズムの決定を参照してください。

ステップ 8 フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される [暗号化アルゴリズム（Encryption Algorithm）] を選択します。

IKEv2 プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、管理対象デバイスによってサポートされているアルゴリズムだけを選択できます。VPN トポロジのエクストラネットのデバイスでは、両方のピアに一致するアルゴリズムを選択する必要があります。VPN で許可するアルゴリズムすべてを選択します。オプションの説明の詳細については、使用する暗号化アルゴリズムの決定を参照してください。

ステップ 9 [PRF アルゴリズム（PRF Algorithm）] を選択します。

IKE ポリシーで使用するハッシュ アルゴリズムの疑似乱数関数部分。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。VPN で許可するアルゴリズムすべてを選択します。オプションの説明の詳細については、使用するハッシュ アルゴリズムの決定を参照してください。

ステップ 10 [DH グループ（DH Group）] を選択し、[追加（Add）] します。

暗号化に使用される Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。VPN で許可するグループを選択します。オプションの説明の詳細については、使用する Diffie-Hellman 係数グループの決定を参照してください。

ステップ 11 [Save] をクリックします。
任意の有効な組み合わせが選択された場合、新しい IKEv2 ポリシーがリストに追加されます。選択されなかった場合、エラーが表示され、このポリシーを正常に保存するために、変更する必要があります。

Firepower Threat Defense IPsec プロポーザル

IPsecプロポーザル（またはトランスフォームセット）はVPNトポロジを設定するときに使用されます。ピアは、ISAKMPとのIPsecセキュリティアソシエーションのネゴシエート中に、特定のデータフローを保護する特定のプロポーザルの使用に同意します。プロポーザルは、両方のピアで同じである必要があります。

IKEバージョン（IKEv1またはIKEv2）に基づいて、別個のIPsecプロポーザルオブジェクトがあります。

- IKEv1 IPsecプロポーザル（またはトランスフォームセット）オブジェクトを作成する場合、IPsecが動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPNで複数の組み合わせをサポートするには、複数のIKEv1 IPsecプロポーザルオブジェクトを作成します。
- IKEv2 IPsecプロポーザルオブジェクトを作成する際に、VPNで許可するすべての暗号化アルゴリズムとハッシュアルゴリズムを選択できます。IKEv2ネゴシエーション中に、ピアは、それぞれでサポートされる最適なオプションを選択します。

カプセル化セキュリティプロトコル（ESP）は、IKEv1とIKEv2の両方のIPsecプロポーザルに使用されます。これは認証、暗号化、およびアンチリプレイサービスを提供します。ESPは、IPプロトコルタイプ50です。

（注） IPsecトンネルで暗号化と認証の両方を使用することを推奨します。

IKEv1 IPsecプロポーザルオブジェクトの設定

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）
エクスポートコンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

手順

ステップ1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IPsec IKev1 プロポーザル（IPsec IKev1 Proposal）]** を選択します。

前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセスレベルによっては、プロポーザルを編集（）、表示（）、または削除（）することもできます。

ステップ2 [IPsec IKEv1プロポーザルの追加（Add IPsec IKEv1 Proposal）]を選択して、新しいプロポーザルを作成します。

ステップ 3 このプロポーザルの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このプロポーザルの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [ESP 暗号化（ESP Encryption）] 方法を選択します。このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。

IKEv1 では、いずれかのオプションを選択します。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。オプションの説明の詳細については、使用する暗号化アルゴリズムの決定を参照してください。

ステップ 6 [ESP ハッシュ（ESP Hash）] のオプションを選択します。

オプションの説明の詳細については、使用するハッシュ アルゴリズムの決定を参照してください。

ステップ 7 [Save] をクリックします。
新しいプロポーザルがリストに追加されます。

IKEv2 IPsec プロポーザル オブジェクトの設定

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）
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択し、目次で **[VPN]** > **[IKEv2 IPsec プロポーザル（IKEv2 IPsec Proposal）]** を選択します。

前に設定したプロポーザルは、システムによって定義されるデフォルトにリストされています。アクセス レベルによっては、プロポーザルを編集（）、表示（）、または削除（）することもできます。

ステップ 2 [IKEv2 IPsec プロポーザルの追加（Add IKEv2 IPsec Proposal）] を選択して、新しいプロポーザルを作成します。

ステップ 3 このプロポーザルの [名前（Name）] を入力します。

ポリシー オブジェクトの名前。最大 128 文字を使用できます。

ステップ 4 このプロポーザルの [説明（Description）] を入力します。

ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

ステップ 5 [ESP ハッシュ（ESP Hash）] 方法を選択して、ハッシュまたは整合性アルゴリズムを認証用プロポーザルに使用します。

IKEv2 では、[ESP ハッシュ（ESP Hash）] をサポートするオプションすべてを選択します。オプションの説明の詳細については、使用するハッシュ アルゴリズムの決定を参照してください。

ステップ 6 [ESP 暗号化（ESP Encryption）] 方法を選択します。このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。

IKEv2 では、[選択（Select）] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。IPsec プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN内のデバイスによってサポートされているアルゴリズムだけを選択できます。オプションの説明の詳細については、使用する暗号化アルゴリズムの決定を参照してください。

ステップ 7 [Save] をクリックします。
新しいプロポーザルがリストに追加されます。

Firepower Threat Defense グループ ポリシー オブジェクト

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、リモート アクセス VPN のエクスペリエンスを定義します。たとえば、グループ ポリシー オブジェクトで、アドレス、プロトコル、接続設定などの一般的な属性を設定します。

ユーザに適用されるグループ ポリシーはVPN トンネルが確立される際に決定されます。RADIUS 承認サーバがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

（注） Firepower Threat Defense ではグループ ポリシー属性の継承はありません。ユーザについては、グループ ポリシー オブジェクトが全体として使用されます。ログイン時に AAA サーバで特定されたグループ ポリシー オブジェクトが使用されるか、またはこれが指定されていない場合は、VPN 接続に対して設定されたデフォルトのグループ ポリシーが使用されます。指定されたデフォルトのグループ ポリシーはデフォルト値に設定できますが、これは、接続プロファイルに割り当てられ、他のグループ ポリシーがユーザに対して特定されていない場合にのみ使用されます。

関連トピック

グループ ポリシー オブジェクトの設定 （112 ページ）

グループ ポリシー オブジェクトの設定

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）
エクスポート制御機能が有効になっている、スマート ライセンス アカウントに関連付けられている AnyConnect ライセンスのいずれか： • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	Firepower Threat Defense	任意（Any）	管理者（Administrator）

Firepower Threat Defense グループ ポリシー オブジェクト （111 ページ）を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]** を選択します。

以前に設定したポリシーがシステム デフォルトと共にリストされます。ユーザのアクセス レベルに応じて、グループ ポリシーの編集、表示、または削除ができます。

ステップ 2 [グループ ポリシーの追加（Add Group Policy）] をクリックするか、現在のポリシーを選択して編集します。

ステップ 3 このポリシーの [名前（Name）] とオプションで [説明（Description）] を入力します。

名前には最大 64 文字の長さを使用でき、スペースも使用できます。説明には、最大 1,024 文字を使用できます。

ステップ 4 グループ ポリシー一般オプション （113 ページ）の説明に従って、このグループ ポリシーの [General] パラメータを指定します。

ステップ 5 グループ ポリシー AnyConnect オプション （114 ページ）の説明に従って、このグループ ポリシーの [AnyConnect] パラメータを指定します。

ステップ 6 グループ ポリシーの詳細オプション （117 ページ）の説明に従って、このグループ ポリシーの [詳細（Advanced）] パラメータを指定します。

ステップ 7 [保存（Save）] をクリックします。
新しいグループ ポリシーがリストに追加されます。

次のタスク

グループ ポリシー オブジェクトをリモート アクセス VPN 接続プロファイルに追加します。

関連トピック

Firepower Threat Defense リモート アクセス VPN 接続プロファイルの追加と編集

グループ ポリシー一般オプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]、[グループ ポリシーの追加（Add Group Policy）] をクリックするか、現在のポリシーを選択して編集します。 をクリックして、[一般（General）] タブを選択します。

VPN プロトコル フィールド

このグループ ポリシーを適用するときに使用できるリモート アクセス VPN トンネルのタイプを指定します。[SSL] または [IPsec IKEv2]

バナー フィールド

ログイン時にユーザに対して表示するバナー テキストを指定します。長さは最大 491 文字です。デフォルト値はありません。IPsec VPN クライアントではバナーに対してすべての HTML がサポートされますが、AnyConnect クライアントでは一部の HTML のみがサポートされます。バナーがリモート ユーザに正しく表示されるようにするには、IPsec クライアントに /n タグ、SSL クライアントに
 タグを使用します。

DNS/WINS フィールド

Domain Naming System（DNS）サーバおよび Windows Internet Naming System（WINS）サーバ。AnyConnect クライアントの名前解決に使用されます。

- [プライマリ DNS サーバ（Primary DNS Server）] および [セカンダリ DNS サーバ（Secondary DNS Server）]：このグループで使用する DNS サーバの IPv4 または IPv6 アドレスを定義するネットワーク オブジェクトを選択または作成します。
- [プライマリ WINS サーバ（Primary WINS Server）] および [セカンダリ WINS サーバ（Secondary WINS Server）]：このグループで使用する WINS サーバの IP アドレスを含むネットワーク オブジェクトを選択または作成します。
- [DHCP ネットワーク範囲（DHCP Network Scope）]：このグループの DHCP ネットワークの IPv4 アドレスを含むネットワーク オブジェクトを選択または作成します。この設定では、IPv6、アドレス範囲、またはサブネット仕様はサポートされていません。適切に設定されていない場合、VPN ポリシーの展開は失敗します。
- [デフォルト ドメイン（Default Domain）]：デフォルト ドメインの名前。最上位ドメイン（たとえば、**example.com**）を指定します。

スプリット トンネリング フィールド

スプリット トンネリングは、一部のネットワーク トラフィックを VPN トンネルに誘導して通過させ（暗号化）、残りのネットワーク トラフィックを VPN トンネルの外に誘導します（非暗号化、つまり「クリア テキストの状態」）。

- [IPv4 スプリット トンネリング/IPv6 スプリット トンネリング（IPv4 Split Tunneling/IPv6 Split Tunneling）]：デフォルトでは、スプリット トンネリングは無効です。IPv4 と IPv6 両方とも、[トンネル上ですべてのトラフィックを許可する（Allow all traffic over tunnel）] に設定されています。このままにした場合、エンドポイントからのすべてのトラフィックは VPN 接続経由で送信されます。

  スプリット トンネリングを設定するには、[次に指定されたトンネル ネットワーク（Tunnel networks specified below）] または [次に指定されたネットワークを除外（Exclude networks specified below）] を選択します。その後、そのポリシーのアクセス コントロール リストを設定します。

- [スプリット トンネル ネットワーク リスト タイプ（Split Tunnel Network List Type）]：使用するアクセス リストのタイプを選択します。[標準アクセス リスト（Standard Access List）] または [拡張アクセス リスト（Extended Access List）] を選択するか、作成します。詳細については、アクセス リスト （96 ページ）を参照してください。

- [DNS 要求スプリット トンネリング（DNS Request Split Tunneling）]：スプリット DNS とも呼ばれます。ご使用の環境で期待される DNS 動作を設定します。

  デフォルトでは、スプリット DNS は無効で、[スプリット トンネル ポリシーに従って DNS 要求を送信する（Send DNS request as per split tunnel policy）] に設定されています。[DNS 要求を常にトンネル経由で送信する（Always send DNS request over tunnel）] を選択すると、すべての DNS 要求は強制的にトンネル経由でプライベート ネットワークに送信されます。

  スプリット DNS を設定するには、[指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）] を選択し、ドメイン名のリストを [ドメイン リスト（Domain List）] フィールドに入力します。これらの要求が、プライベート ネットワークにスプリット トンネルを介して解決されます。他のすべての名前は、パブリック DNS サーバを使用して解決されます。ドメインのリストに最大 10 のエントリをカンマで区切って入力します。文字列全体は、255 文字以下である必要があります。

関連トピック

グループ ポリシー オブジェクトの設定 （112 ページ）

グループ ポリシー AnyConnect オプション

これらの仕様は、AnyConnect VPN クライアントの動作に適用されます。

ナビゲーション

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]。[グループ ポリシーの追加（Add Group Policy）] をクリックする

か、現在のポリシーを選択して編集します。次に、[AnyConnect（AnyConnect）] タブを選択します。

プロファイル フィールド

[プロファイル（Profile）]：AnyConnect クライアント プロファイル を含むファイル オブジェクトを選択または作成します。オブジェクト作成の詳細については、Firepower Threat Defense ファイル オブジェクト （118 ページ）を参照してください。

AnyConnect クライアント プロファイルは XML ファイルに格納された設定パラメータのグループです。AnyConnect ソフトウェア クライアントは、クライアントのユーザ インターフェイスに表示される接続エントリを設定するためにこれを使用します。これらのパラメータ（XML タグ）では、追加の AnyConnect 機能を有効にする設定も行われます。

AnyConnect クライアント プロファイル を作成するには、独立した構成ツールである GUI ベースの AnyConnect プロファイル エディタ を使用します。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの *AnyConnect* プロファイル エディタ の章を参照してください。

SSL 設定フィールド

- [SSL 圧縮（SSL Compression）]：データ圧縮を有効にするかどうか。有効にする場合は、使用するデータ圧縮の方法（[圧縮（Deflate）] または [LZS（LZS）]）。[SSL 圧縮（SSL Compression）] はデフォルトで無効になっています。

  データ圧縮は、伝送速度を上げますが、各ユーザ セッションのメモリ要件と CPU 使用率も高めます。そのため、セキュリティ アプライアンスの全体的なスループットが低下します。

- [DTLS 圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）の接続を圧縮するかどうか。[DTLS 圧縮（DTLS Compression）] はデフォルトで無効になっています。

- [MTU サイズ（MTU Size）]：Cisco AnyConnect VPN クライアントによって確立された SSL VPN 接続の最大伝送単位（MTU）サイズ。デフォルトは 1406 バイト、有効な範囲は 576 ～ 1462 バイトです。

  - [DF ビットを無視（Ignore DF Bit）]：フラグメント化が必要なパケットの Don't Fragment（DF）ビットを無視するかどうか。DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。

接続設定フィールド

- [AnyConnect クライアントと VPN ゲートウェイ間のキープアライブ メッセージの有効化（Enable Keepalive Messages between AnyConnect Client and VPN gateway）] およびその [間隔（Interval）] 設定：トンネルでのデータ送受信にピアを使用できることを示すために、ピア間でキープアライブ メッセージを交換するかどうかを指定します。デフォルトでは有効です。キープアライブ メッセージは、設定された間隔で送信されます。有効にする場合

は、リモート クライアントが IKE キープアライブ パケットの各送信間の待機時間の間隔を入力します（秒単位）。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。

- [デッド ピア検出の有効化（Enable Dead Peer Detection）] およびその [間隔（Interval）] 設定：デッド ピア検出（DPD）により、VPN セキュア ゲートウェイまたは VPN クライアントは、ピアが応答しなくなったこと、および接続に失敗したことを迅速に検出できます。デフォルトでは、ゲートウェイとクライアントの両方で有効です。DPD メッセージは、設定された間隔で送信されます。有効にする場合は、リモート クライアントが DPD メッセージの各送信間の待機時間の間隔を入力します（秒単位）。デフォルトの間隔は 30 秒、有効な範囲は 5 ～ 3600 秒です。

- [クライアント バイパス プロトコルを有効にする（Enable Client Bypass Protocol）]：セキュア ゲートウェイが IPv6 トラフィックだけを想定しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを想定しているときの IPv6 トラフィックの管理方法を設定することができます。

  AnyConnect クライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合に、ヘッドエンドが IP アドレスを割り当てなかったネットワーク トラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できるようになりました。

  たとえば、セキュア ゲートウェイが AnyConnect 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアル スタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [SSL キー再生成（SSL rekey）]：クライアントが接続のキーを再生成できるようにして、暗号キーと初期化ベクターを再ネゴシエートし、接続のセキュリティを向上させます。これは、デフォルトでは無効になっています。有効にすると、再ネゴシエーションが指定された間隔で実行され、既存のトンネルのキーが再生成されるか、次のフィールドを設定して新しいトンネルが作成されます。

  - [方法（Method）]：SSL キー再生成が有効な場合に使用可能です。[新しいトンネル（New Tunnel）] を作成する（デフォルト）か、[既存のトンネル（Existing Tunnel）] の仕様を再ネゴシエーションします。

  - [間隔（Interval）]：SSL キー再生成が有効な場合に使用可能です。4 ～ 10080 分（1 週間）の範囲で 4 分のデフォルトに設定します。

- [クライアント ファイアウォール ルール（Client Firewall Rules）]：クライアント ファイアウォール ルールを使用して VPN クライアントのプラットフォームのファイアウォール設定を設定します。ルールは、送信元アドレス、宛先アドレス、プロトコルなどの条件に基づきます。拡張アクセス コントロール リスト構成要素オブジェクトを使用してトラフィックのフィルタ条件を定義します。このグループ ポリシーの拡張 ACL を選択するか、作成します。プライベート ネットワークに流れるデータを制御する [プライベート ネットワー

ク ルール（Private Network Rule）]、確立された VPN トンネルの外部に「クリア テキストで」流れるデータを制御する [パブリック ネットワーク ルール（Public Network Rule）]、または両方を定義します。

（注） ACL に TCP/UDP/ICMP/IP ポートのみが含まれていて、送信元ネットワークが any、any-IPv4、または any-IPv6 であることを確認します。

Microsoft Windows を実行している VPN クライアントだけが、これらのファイアウォール設定を使用できます。

関連トピック

グループ ポリシー オブジェクトの設定 （112 ページ）

グループ ポリシーの詳細オプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [グループ ポリシー（Group Policy）]、[グループ ポリシーの追加（Add Group Policy）] をクリックするか、現在のポリシーを選択して編集します。 をクリックし、[詳細設定（Advanced）] タブを選択します。

トラフィック フィルタ フィールド

- [アクセス リスト フィルタ（Access List Filter）]：フィルタは、VPN 接続を経由するトンネリングされたデータ パケットを許可するかブロックするかを決定するルールで構成されています。ルールは、送信元アドレス、宛先アドレス、プロトコルなどの基準に基づいています。拡張アクセスコントロールリストの構成要素オブジェクトは、トラフィック フィルタ基準を定義するために使用されます。このグループ ポリシーの新しい拡張 ACL を選択または作成します。
- [VPN を VLAN に規制する（Restrict VPN to VLAN）]：「VLAN マッピング」とも呼ばれ、このパラメータにより、このグループ ポリシーが適用されるセッションの出力 VLAN インターフェイスが指定されます。ASA は、このグループからのすべてのトラフィックを指定された VLAN に転送します。

  この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。ドロップダウン リストには、デフォルト値（[無制限（Unrestricted）]）の他に、この ASA で設定されている VLAN だけが表示されます。可能な値の範囲は 1 ～ 4094 です。

セッション設定フィールド

- [アクセス時間（Access Hours）]：時間範囲オブジェクトを選択または作成します。このオブジェクトは、このグループ ポリシーがリモート アクセス ユーザに適用可能な時間範囲を指定します。詳細については、時間範囲オブジェクト （25 ページ）を参照してください。
- [ユーザあたり同時ログイン（Simultaneous Logins Per User）]：ユーザに許可する同時ログインの最大数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインが無効になり、ユーザ アクセスを禁止します。複数の同時接続を許可した場合、セキュリティの重大な問題が発生し、パフォーマンスに影響する可能性があります。
- [最大接続時間（Maximum Connection Time）]/[アラート間隔（Alert Interval）]：最大ユーザ接続時間（分単位）を指定します。ここで指定した時間が経過すると、システムは接続を停止します。最小値は 1 分です。[アラート間隔（Alert Interval）] では、最大接続時間に達してユーザにメッセージを表示するまでの時間間隔を指定します。
- [アイドル タイムアウト（Idle Timeout）]/[アラート間隔（Alert Interval）]：このユーザのアイドル タイムアウト期間（分単位）を指定します。この期間、ユーザ接続に通信アクティビティがなかった場合、システムは接続を停止します。最小値は 1 分です。デフォルトは 30 分です。[アラート間隔（Alert Interval）] では、アイドル時間に達してユーザにメッセージを表示するまでの時間間隔を指定します。

関連トピック

グループ ポリシー オブジェクトの設定 （112 ページ）

Firepower Threat Defense ファイル オブジェクト

[ファイル オブジェクトの追加（Add File Object）] や [ファイル オブジェクトの編集（Edit File Object）] ダイアログボックスを使用して、ファイル オブジェクトを作成および編集します。ファイル オブジェクトは、通常はリモート アクセス VPN ポリシーの設定で使用するファイルを表します。これには、AnyConnect クライアント プロファイル ファイルや AnyConnect クライアントイメージ ファイルが含まれます。

ファイル オブジェクトを作成すると、Firepower Management Center によってそのファイルのコピーがリポジトリに作成されます。これらのファイルは、データベースのバックアップを作成するたびにバックアップされ、データベースを復元すると復元されます。ファイルオブジェクトでの使用のためにファイルを Firepower Management Center プラットフォームにコピーするときは、ファイルをファイル リポジトリに直接コピーしないでください。

ファイル オブジェクトを削除しても、関連付けられているファイルはファイル リポジトリから削除されず、オブジェクトのみが削除されます。

ファイルオブジェクトを指定する設定を展開すると、関連付けられているファイルが、該当するディレクトリのデバイスにダウンロードされます。

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）]。

フィールド

- [名前（Name）] と [説明（Description）]：最大 128 文字の名前を入力し、オプションでこのファイル オブジェクトを識別するための説明を入力します。
- [ファイル名（File Name）] と [ファイル タイプ（File Type）]：ファイルの名前とフルパス、およびタイプ。[参照（Browse）] をクリックしてファイルを選択し、該当するタイプをクリックします。

  ファイル オブジェクトに含めるためには **AnyConnect クライアントイメージ** および **AnyConnect クライアント プロファイル** タイプのみが有効で、Firepower Management Center プラットフォームに存在する必要があります。

関連トピック

Cisco AnyConnect セキュア モビリティ クライアント イメージについてFirepower Threat Defense
グループ ポリシー AnyConnect オプション （114 ページ）

Firepower Threat Defense 証明書のマップ オブジェクトについて

証明書のマップ オブジェクトは、証明書一致ルールの名前付きセットです。これらのオブジェクトは、受信した証明書とリモート アクセス VPN 接続プロファイルとの関連付けを提供するために使用されます。接続プロファイルと証明書のマップ オブジェクトは両方とも、リモート アクセス VPN ポリシーの一部です。受信した証明書が証明書マップに含まれているルールと一致すると、接続は指定の接続プロファイルに「マッピングされている」か、関連付けられています。ルールは優先順位で整理され、UI に表示される順序で照合されます。照合は、証明書マップ オブジェクト内の最初のルールが一致したときに終了します。

ナビゲーション

[オブジェクト（Objects）] > [オブジェクトの管理（Object Management）] > [VPN] > [証明書のマップ（Certificate Map）]

フィールド

- [名前（Name）]：このオブジェクトを特定します。これにより、リモート アクセス VPN などの他の設定で参照できます。
- [マッピング条件（Mapping Criteria）]：評価する証明書の内容を指定します。証明書がこれらのルールの条件を満たしている場合、ユーザはこのオブジェクトを含む接続プロファイルにマッピングされます。
  - [コンポーネント（Component）]：一致ルールに対して使用するクライアント証明書のコンポーネントを選択します。

- [フィールド（Field）]：クライアント証明書の [件名（Subject）] または [発行元（Issuer）] に従って、一致ルールのフィールドを選択します。

  [フィールド（Field）] が [代替サブジェクト（Alternative Subject）] または [拡張キーの使用状況（Extended Key Usage）] に設定されている場合、コンポーネントは [フィールド全体（Whole Field）] として凍結されます。

- [演算子（Operator）]：一致ルールの演算子を次のうちから選択します。
  - [等しい（Equals）]：証明書コンポーネントは、入力された値と一致する必要があります。完全に一致しない場合、接続は拒否されます。
  - [含む（Contains）]：証明書コンポーネントには、入力された値が含まれている必要があります。コンポーネントにその値が含まれていない場合、接続は拒否されます。
  - [等しくない（Does Not Equal）]：証明書コンポーネントは、入力された値と等しくない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値が US と等しければ、接続が拒否されます。
  - [次を含まない（Does Not Contain）]：証明書コンポーネントには、入力された値が含まれていない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値に US が含まれていると、接続が拒否されます。

- [値（Value）]：一致ルールの値。入力された値は、選択されたコンポーネントおよび演算子と関連付けられています。

関連トピック

証明書マップの設定

アドレス プール

クラスタリングの Diagnostic インターフェイス、または VPN リモート アクセス プロファイルに使用できる IPv4 および IPv6 の両方で、IP アドレス プールを設定できます。

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
任意	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）] > [IPv4 プール（IPv4 Pools）]** を選択します。

ステップ 2 [IPv4 プールを追加（Add IPv4 Pools）] をクリックし、次のフィールドを設定します。

- [名前（Name）]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [説明（Description）]：このプールのオプションの説明を追加します。
- [IP アドレス（IP Address）]：プールで使用できるアドレスの範囲を入力します。ドット付き 10 進表記および最初と最後のアドレスの間でハイフンを使用します。例：10.10.147.100-10.10.147.177。
- [マスク（Mask）]：この IP アドレスプールが常駐するサブネットを指定します。
- [オーバーライドを許可（Allow Overrides）]：このチェックボックスをオンにして、オブジェクトのオーバーライドを有効にします。展開矢印をクリックして、[オーバーライド（Overrides）]テーブルを表示します。[追加（Add]）をクリックして、新たなオーバーライドを追加することができます。詳細については、オブジェクトのオーバーライド（9 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [IPv6 プールの追加（Add IPv6 Pools）] をクリックし、次のフィールドを設定します。

- [名前（Name）]：アドレス プールの名前を入力します。最大 64 文字を指定できます。
- [説明（Description）]：このプールのオプションの説明を追加します。
- [IPv6 アドレス（IPv6 Address）]：設定されたプールで使用できる最初の IP アドレスとビットのプレフィックス長を入力します。たとえば、2001:DB8::1/64 となります。
- [アドレスの数（Number of Addresses）]：開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。
- [オーバーライドを許可（Allow Overrides）]：このチェックボックスをオンにして、オーバーライドを有効にします。展開矢印をクリックして、[オーバーライド（Overrides）] テーブルを表示します。[追加（Add]）をクリックして、新たなオーバーライドを追加することができます。詳細については、オブジェクトのオーバーライド（9 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

FlexConfig オブジェクト

FlexConfig ポリシーで FlexConfig ポリシー オブジェクトを使用して、他の方法では Firepower Management Center を使用して設定できない Firepower Threat Defense デバイスの機能のカスタマイズされた設定を指定します。FlexConfig ポリシーの詳細については、FlexConfig ポリシーの概要を参照してください。

FlexConfig の次のタイプのオブジェクトを設定できます。

テキスト オブジェクト

テキスト オブジェクトは、FlexConfig オブジェクトで変数として使用する自由形式のテキスト文字列を定義します。このオブジェクトに単一の値を設定したり、このオブジェクトを複数の値のリストにしたりすることができます。

事前定義済みの FlexConfig オブジェクトで使用される複数の事前定義済みテキスト オブジェクトがあります。関連付けられている FlexConfig オブジェクトを使用する場合は、単に、テキスト オブジェクトの内容を編集して、FlexConfig オブジェクトによる特定のデバイスの設定方法をカスタマイズすることだけが必要です。事前定義済みのオブジェクトを編集するには、一般に、これらのオブジェクトのデフォルト値を直接変更するのではなく、設定しているデバイスごとにデバイスの上書きを作成することをお勧めします。これは、他のユーザが別の一連のデバイスに同じ FlexConfig オブジェクトを使用する場合に、意図しない結果が発生しないようにするのに役立ちます。

テキスト オブジェクトの設定については、FlexConfig テキスト オブジェクトの設定を参照してください。

FlexConfig オブジェクト

FlexConfig オブジェクトには、デバイス設定コマンド、変数、およびスクリプト言語の手順が含まれています。導入展開時に、これらの手順が処理されて、一連の設定コマンドが、ターゲット デバイスで特定の機能を設定するカスタマイズされたパラメータとともに作成されます。

これらの手順は、通常の Firepower Management Center ポリシーで定義されている機能が設定される前（先頭に付加）または後（付加）に設定されます。Firepower Management Center で設定されたオブジェクト（ネットワーク オブジェクトなど）に依存する FlexConfig は、設定展開に付加される必要があります。付加されない場合、必要なオブジェクトが、FlexConfig がこのオブジェクトを参照する必要がある前に設定されません。

FlexConfig オブジェクトの設定の詳細については、FlexConfig オブジェクトの設定を参照してください。

RADIUS サーバ グループ

RADIUS サーバ グループ オブジェクトには、RADIUS サーバへの参照が 1 つ以上含まれています。これらの AAA サーバは、リモート アクセス VPN 接続を通じてユーザのログインを認証するために使用されます。

始める前に

（注） RADIUS サーバ グループ オブジェクトは、オーバーライドできません。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [RADIUS サーバ グループ（RADIUS Server Group）]** を選択します。

現在設定されているすべての RADIUS サーバ グループ オブジェクトがリスト表示されます。フィルタを使用して、リストを絞り込んでください。

ステップ 2 リストされた [RADIUS サーバ グループ（RADIUS Server Group）] オブジェクトを選択し、編集するか、新しいオブジェクトを追加します。

このオブジェクトを設定する場合は、RADIUS サーバ オプション （124 ページ）およびRADIUS サーバ グループのオプション （123 ページ）を参照してください。

ステップ 3 [Save] をクリックします。

RADIUS サーバ グループのオプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [RADIUS サーバ グループ（RADIUS Server Group）]。設定済みの RADIUS サーバ グループ オブジェクトを選択して編集するか、または新しく追加します。

フィールド

- [名前（Name）] と [説明（Description）]：この RADIUS サーバ グループ オブジェクトを識別するための名前と、任意で説明を入力します。
- [許可のみを有効にする（Enable authorize only）]：この RADIUS サーバ グループが認証に使用されないが、許可またはアカウンティングに使用される場合は、このフィールドをオンにすると RADIUS サーバ グループの許可限定モードが有効になります。

  許可限定モードでは、アクセス要求に RADIUS サーバ パスワードを含める必要がありません。したがって、個別の RADIUS サーバに設定されたパスワードが無視されます。
- [アカウントの暫定更新（Enable interim account update）を有効にする] および [間隔（Interval）]：新たに割り当てられた IP アドレスを RADIUS サーバに通知するために、RADIUS interim-accounting-update メッセージの生成を有効にします。[間隔（Interval）]

フィールドの定期アカウンティング更新の間隔時間長を設定します。有効数は 1 ～ 120 であり、デフォルト値は 24 です。

- [グループ アカウンティング モード（Group Accounting Mode）]：グループ内の RADIUS サーバにアカウンティング メッセージを送信するための方法です。[1 つ（Single）] を選択します。アカウンティング メッセージがグループ内の 1 つのサーバに送信されます。これはデフォルトです。または、[同時（Simultaneous）] を選択します。アカウンティング メッセージがグループ内のすべてのサーバに同時に送信されます。
- [間隔のリトライ（Retry Interval）]：RADIUS サーバへの接続を試みる間隔です。間隔の範囲は、1 ～ 10 秒です。
- [レルム（Realms）]（オプション）：この RADIUS サーバ グループに関連付ける AD または LDAP レルムを指定または選択します。その後、トラフィック フローの VPN 認証アイデンティティ ソースの判別時に、関連する RADIUS サーバ グループにアクセスするためにこのレルムがアイデンティティ ポリシーで選択されます。このレルムは実質的に、アイデンティティ ポリシーからこの Radius サーバ グループへのブリッジを提供します。この RADIUS サーバ グループにレルムを関連付けない場合、アイデンティティ ポリシーでトラフィック フローの VPN 認証アイデンティティ ソースを判別するために RADIUS サーバ グループに到達することができません。
- [RADIUS サーバ（RADIUS Servers）]：を参照。 RADIUS サーバ オプション （124 ページ）

関連トピック

RADIUS サーバ グループ （122 ページ）

RADIUS サーバ オプション

ナビゲーション パス

[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [RADIUS サーバ グループ（RADIUS Server Group）]。リストされた [RADIUS サーバ グループ（RADIUS Server Group）] オブジェクトを選択し、編集するか、新しいオブジェクトを追加します。次に、[RADIUS サーバ グループ（RADIUS Server Group）] ダイアログで、リストされた RADIUS サーバを選択して、編集するか、新しい RADIUS サーバを追加します。

フィールド

- [名前（Name）] および [説明（Description）]：この RADIUS サーバ オブジェクトを識別するには、名前（128 文字以下）と必要に応じて説明を入力します。
- [ホスト名/IP アドレス（Hostname/IP Address]：認証要求が送信される RADIUS サーバのホスト名または IP アドレスを特定するネットワーク オブジェクトです。ホスト名または IP アドレスを 1 つのみ選択し、追加のサーバに追加し、更なる RADIUS サーバを RADIUS サーバ グループ リストに追加します。

- [認証ポート（Authentication Port）]：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [キー（Key）] および [キーの確認（Confirm Key）]：管理対象デバイス（クライアント）と RADIUS サーバ間でデータを暗号化するために使用される共有秘密です。

  キーでは、127 文字以下の英数字で、大文字と小文字を区別します。特殊文字も使用可能です。

  このフィールドで定義したキーは、RADIUS サーバのキーと一致している必要があります。確認フィールドでもう一度キーを入力します。
- [アカウンティング ポート（Accounting Port）]：RADIUS アカウンティングが実行されるポートです。デフォルトは 1813 です。

関連トピック

RADIUS サーバ グループ （122 ページ）
RADIUS サーバ グループのオプション （123 ページ）