オブジェクト管理

この章では、再利用可能なオブジェクトを管理する方法について説明します。

- オブジェクトの概要 （2 ページ）
- オブジェクト マネージャ （5 ページ）
- AAAサーバ （15 ページ）
- アクセスリスト （22 ページ）
- アドレス プール （29 ページ）
- アプリケーション フィルタ （31 ページ）
- ASパス （32 ページ）
- BFD テンプレート （33 ページ）
- 暗号スイート リスト （34 ページ）
- コミュニティ リスト （35 ページ）
- DHCP IPv6 プール （39 ページ）
- 識別名 （39 ページ）
- DNS サーバ グループ （42 ページ）
- 外部属性 （43 ページ）
- ファイル リスト （51 ページ）
- FlexConfig （57 ページ）
- 位置情報 （58 ページ）
- インターフェイス（Interface） （59 ページ）
- Key Chain （59 ページ）
- ネットワーク （62 ページ）
- PKI （66 ページ）
- ポリシー リスト （87 ページ）
- ポート （89 ページ）
- プレフィックス リスト （91 ページ）
- ルート マップ （93 ページ）
- セキュリティ インテリジェンス （98 ページ）
- シンクホール （111 ページ）
- SLA モニタ （112 ページ）

• 時間範囲 （114 ページ）
• タイムゾーン （116 ページ）
• トンネル ゾーン （116 ページ）
• URL （117 ページ）
• 変数セット （119 ページ）
• VLAN タグ （136 ページ）
• VPN （137 ページ）
• オブジェクト管理の履歴 （161 ページ）

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、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。

- ネットワーク、ポート、VLAN、またはURLオブジェクトが使用されているポリシー、設定、およびその他のオブジェクトを表示します。オブジェクトとその使用状況の表示 （9 ページ）を参照してください。
- 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 （10 ページ）を参照してください。
- 選択したデバイスのオブジェクト値を上書きします。オブジェクトのオーバーライド （12 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。

（注） オブジェクトは、そのデバイスに割り当てられているポリシーでオブジェクトが使用される場合のみ、管理対象デバイスで設定されます。特定のデバイスに割り当てられているすべてのポリシーからオブジェクトを削除する場合、オブジェクトは、次の導入時にデバイス設定からも削除され、オブジェクトに対する後続の変更はデバイス設定に反映されません。

オブジェクト タイプ

次の表に、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	○	○
[ポート（Port）]	○	○
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	いいえ	いいえ
トンネル ゾーン	いいえ	いいえ
アプリケーション フィルタ	いいえ	いいえ
VLAN タグ	○	○
外部属性：セキュリティグループタグ（SGT）およびダイナミックオブジェクト	いいえ	いいえ
URL	○	○
位置情報（GeoLocation）	いいえ	いいえ
時間範囲	いいえ	いいえ
変数セット	いいえ	いいえ
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	いいえ	いいえ
シンクホール	いいえ	いいえ
ファイル リスト	いいえ	いいえ
暗号スイート リスト	いいえ	いいえ
識別名（Distinguished Name）	はい	いいえ
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	はい	いいえ
キーチェーン	いいえ	はい

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
DNS サーバー グループ	いいえ	いいえ
SLA モニター	いいえ	いいえ
プレフィックス リスト：IPv4 および IPv6	いいえ	はい
ルート マップ	いいえ	はい
アクセス リスト：標準および拡張	いいえ	はい
AS パス	いいえ	はい
コミュニティ リスト（Community List）	いいえ	はい
ポリシー リスト	いいえ	はい
FlexConfig：テキストおよびFlexConfig オブジェクト	いいえ	はい

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ーは、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、**Refresh** ( ) をクリック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。ページのオブジェクトは、名前または値でフィルタ処理できます。

オブジェクトのインポート

オブジェクトは、カンマ区切り値ファイルからインポートできます。1回の試行で最大1000個のオブジェクトをインポートできます。カンマ区切り値ファイルの内容は、特定の形式に従う必要があります。形式はオブジェクトタイプごとに異なります。一部のタイプのオブジェクトのみをインポートできます。サポートされているオブジェクトタイプと対応するルールについては、次の表を参照してください。

オブジェクト タイプ	ルール

個々のオブジェクト	• 列ヘッダーは大文字で指定する必要があります。
	• ファイルには、次の列ヘッダーが必要です。
	  • NAME
	  • [DN]
	• エントリをインポートするには、NAME 列と DN 列の両方のエントリが必須です。
	• 個々のオブジェクトを既存の識別名オブジェクトグループに直接インポートできます。

オブジェクト タイプ	ルール
ネットワーク オブジェクト	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • DESCRIPTION • タイプ • 値 • LOOKUP • ホスト、範囲、またはネットワーク オブジェクト タイプのエントリをインポートするには、NAME 列と VALUE 列のエントリが必須です。 • FQDN オブジェクトの場合、TYPE 列のエントリは「fqdn」を指定する必要があり、LOOKUP 列エントリは「ipv4」、「ipv6」、または「ipv4_ipv6」を指定する必要があります。 • FQDN オブジェクトの LOOKUP 列エントリに内容が指定されていない場合、オブジェクトは ipv4_ipv6 フィールド値で保存されます。
ポート	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • プロトコル • ポート • ICMPCODE • ICMPTYPE • NAME 列のエントリは必須です。 • 「tcp」および「udp」プロトコルタイプの場合、PORT 列のエントリは必須です。 • 「icmp」および「icmp6」プロトコルタイプの場合、ICMPCODE 列および ICMPTYPE 列のエントリは必須です。

オブジェクト タイプ	ルール
URL	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • DESCRIPTION • URL • エントリをインポートするには、NAME 列と URL 列のエントリが必須です。
VLAN タグ	• 列ヘッダーは大文字で指定する必要があります。 • ファイルには、次の列ヘッダーが必要です。 • NAME • DESCRIPTION • TAG • エントリをインポートするには、NAME 列と TAG 列のエントリが必須です。

手順

ステップ 1 **Objects** > **Object Management** を選択します。

ステップ 2 左ペインから、次のオブジェクトタイプのいずれかを選択します。

- **[識別名（Distinguished Name）]** > **[個々のオブジェクト（Individual Objects）]** >
- **[ネットワーク オブジェクト（Network Object）]**
- **ポート（Port）**
- **URL**
- **VLAN タグ**

ステップ 3 [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 [オブジェクトのインポート（Import Object）] を選択します。

（注）
前の手順で [個々のオブジェクト（Individual Objects）] を選択した場合は、[インポート（Import）] をクリックします。

ステップ 4 [参照（Browse）] をクリックします。

ステップ 5 システム上のカンマ区切りファイルを見つけて選択します。

ステップ 6 [Open] をクリックします。

（注）
識別名オブジェクトをインポートするときに、必要に応じて、[インポートされた識別名オブジェクトを以下のオブジェクトグループに追加する（Add imported Distinguished Name objects to the below object group）] チェックボックスをオンにして、ドロップダウンボックスからグループ名を選択することで、オブジェクトを既存の識別名オブジェクトグループに直接インポートすることができます。

ステップ 7 [インポート（Import）] をクリックします。

オブジェクトの編集

手順

ステップ 1 **Objects** > **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（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**Edit** ( )をクリックします。

代わりに **View** ( ) が表示される場合、オブジェクトは先祖ドメインに属し、オーバーライド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 （133 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、[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 （14 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、[Override]セクションを展開し、[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 （14 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

オブジェクトとその使用状況の表示

[オブジェクト管理（Object Management）]ページで、オブジェクトの使用状況の詳細を表示できます。Firewall Management Center では、多くのオブジェクトタイプに対してこの機能を使用できます。ただし、一部のオブジェクトタイプはサポートされていません。

手順

ステップ 1 **Objects** > **Object Management** を選択します。

ステップ 2 次のいずれかのサポートされているオブジェクトタイプを選択します。

- [アクセスリスト（Access List）] > [拡張（Extended）]
- [アクセスリスト（Access List）] > [標準（Standard）]
- AS パス
- コミュニティ リスト（Community List）
- Interface
- ネットワーク（Network）
- ポリシー リスト
- ポート
- [プレフィックスリスト（Prefix List）] > [IPv4プレフィックスリスト（IPv4 Prefix List）]
- [プレフィックスリスト（Prefix List）] > [IPv6プレフィックスリスト（IPv6 Prefix List）]
- ルートマップ
- SLA モニタ
- URL
- VLAN タグ

ステップ 3 オブジェクトの横にある**Find Usage** ()アイコンをクリックします。

[オブジェクトの使用率（Object Usage）] ウィンドウには、オブジェクトが使用されているすべてのポリシー、オブジェクト、およびその他の設定のリストが表示されます。オブジェクトの使用率の詳細を確認するには、リスト内のいずれかの項目をクリックします。オブジェクト

が使用されるポリシーおよびその他の設定については、対応するリンクをクリックすると、それぞれの UI ページにアクセスすることができます。

オブジェクトまたはオブジェクト グループのフィルタリング

手順

ステップ 1 **Objects** > **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。

次のワイルドカードを使用できます。

- 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。

ステップ 3 [未使用のオブジェクトを表示（Show Unused Object）] チェックボックスをオンにして、システム内のどこでも使用されていないオブジェクトとオブジェクトグループを表示します。

（注）
- オブジェクトが未使用オブジェクトのグループに含まれる場合、そのオブジェクトは使用済みと見なされます。ただし、[未使用のオブジェクトを表示（Show Unused Object）] チェックボックスをオンにすると、未使用オブジェクトのグループが表示されます。
- [未使用のオブジェクトを表示（Show Unused Object）] チェックボックスは、ネットワーク、ポート、URL、および VLAN タグのオブジェクトタイプでのみ使用できます。

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。

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

手順

ステップ 1 **Objects** > **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）] 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（**Search** ()）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**Reload** ()をクリックするか、検索フィールド内の**Clear** ()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、その場でオブジェクトを作成するには、**Add** ()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 （14 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。設定変更の展開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。

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
- 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
- 証明書の登録（PKI）
- キーチェーン

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

手順

ステップ 1 **Objects** > **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（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**Edit** ( )をクリックします。

代わりに **View** ( ) が表示される場合、オブジェクトは先祖ドメインに属し、オーバーライド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（14 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（14 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**Delete** ( )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（15 ページ）を参照）。

オブジェクトのオーバーライドの許可

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 **[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 （14 ページ） を参照）。

オブジェクトのオーバーライドの追加

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 （14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 [Add] をクリックします。

ステップ 3 [ターゲット（Targets）] 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 （任意）[Description] に説明を入力します。

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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

オブジェクト オーバーライドの編集

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 **Edit** (✎) 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

AAAサーバ

再利用可能な AAA サーバーオブジェクトを追加します。

RADIUS サーバーグループの追加

RADIUS サーバー グループ オブジェクトには、RADIUS サーバーへの参照が 1 つ以上含まれています。これらのサーバーは、リモート アクセス VPN 接続を通じてユーザーのログインを認証するために使用されます。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

始める前に

（注） RADIUS サーバー 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 **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** を選択します。

現在設定されているすべての RADIUS サーバー 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 サーバー オプション （18 ページ）およびRADIUS サーバー グループのオプション （16 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。

RADIUS サーバー グループのオプション

ナビゲーション パス

Objects > **Object Management** > **AAA Server** > **RADIUS Server Group**。設定済みの RADIUS サーバー 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 サーバー 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。
- [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 サーバー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 つのサーバーに送信されます。これはデフォルトです。または、[同時（Multiple）] 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ー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 サーバーグループに関連付ける Active Directory（AD）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 サーバー 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 サーバー 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 サーバー グループに到達することができません。

（注） ユーザーアイデンティティと RADIUS をアイデンティティソースとしてリモートアクセス VPN を使用する場合、このフィールドは必須です。

- [許可のみを有効にする（Enable authorize only）]：この RADIUS サーバー 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 サーバー 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 サーバーに通知するために、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。
- [ダイナミック認証の有効化（Enable Dynamic Authorization）] と [ポート（Port）]：この RADIUS サーバ グループの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にします。[ポート（Port）] フィールドで、RADIUS CoA 要求のリスニング ポートを指定します。有効数は 1024 ～ 65535 であり、デフォルト値は 1700 です。一旦定義されると、対応する RADIUS サーバ グループが CoA 通知用に登録され、Cisco Identity Services Engine（ISE）から CoA ポリシーの更新を行うポートにリッスンします。
- [ダウンロード可能ACLとシスコAVペアACLの結合（Merge Downloadable ACL with Cisco AV Pair ACL）]：ダウンロード可能アクセス制御リスト（dACL）とシスコ属性値（AV）ペア ACL の結合を有効にします。

  ダウンロード可能 ACL は、CiscoISE のアクセス制御リストを定義および更新し、該当するすべてのコントローラへの ACL のダウンロードを可能にします。Cisco ISE での dACL の使用の詳細については、『*Cisco ISE Administrator Guide*』にあるセグメンテーションに関する章の認証ポリシーに関するセクションを参照してください。

  シスコ AV ペア ACL を使用して、個々のセッションについて特定の認証、許可、およびアカウンティング要素を定義できます。Cisco ISE での dACL の使用の詳細については、

『*Cisco ISE Administrator Guide*』にあるセグメンテーションに関する章の認証プロファイル設定に関するセクションを参照してください。

[ダウンロード可能ACLとシスコAVペアACLの結合（Merge Downloadable ACL with Cisco AV Pair ACL）] をオンにした場合は、次のオプションを選択できます。

- [シスコAVペアACLの後（After Cisco AV Pair ACL）] は、ダウンロード可能 ACL のエントリを Cisco AV ペアのエントリの後に配置する必要があることを意味します。
- [シスコAVペアACLの前（Before Cisco AV Pair ACL）] は、ダウンロード可能 ACL のエントリを Cisco AV ペアのエントリの前に配置する必要があることを意味します。

- [RADIUSサーバー（RADIUS Servers）]：RADIUS サーバー オプション （18 ページ） を参照してください。

関連トピック

RADIUS サーバーグループの追加 （16 ページ）

RADIUS サーバー オプション

ナビゲーション パス

Objects > **Object Management** > **AAA Server** > **RADIUS Server Group**。リストされた [RADIUS サーバー 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

- [IPアドレス/ホスト名（IP Address/Hostname）]：認証要求が送信される RADIUS サーバーのホスト名または 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。

（注） デバイスは、RADIUS 認証の IPv6 IP アドレスをサポートするようになりました。

- [RADIUSサーバー対応メッセージ オーセンティケータ（RADIUS Server-Enabled Message Authenticator）]：メッセージ オーセンティケータは、サーバーとクライアントの間の通信を保護し、RADIUS サーバーとファイアウォールデバイスの間のセキュアな接続に必要です。メッセージオーセンティケータを無効にすると、ファイアウォールが攻撃にさらされる可能性があります。

  次の点に注意してください。

  - RADIUS サーバーにメッセージ オーセンティケータの設定が必要です。

- メッセージ オーセンティケータをサポートしている、互換性のある Firewall Threat Defense デバイスが必要です。それ以外の場合は、RADIUS ログインが失敗する可能性があります。この機能をサポートしている、互換性のあるFTDの詳細については、RADIUS サーバー対応メッセージ オーセンティケータの互換性マトリックス （20 ページ）を参照してください。

- [認証ポート（Authentication Port）]：RADIUS認証および認可が実行されるポート。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。
- [タイムアウト（Timeout）]：認証のセッション タイムアウト。

（注） RADIUS 二要素認証の場合、タイムアウト値は 60 秒以上必要です。デフォルトのタイムアウト値は 10 秒です。

- [使用して接続（Connect Using）]：ルートルックアップまたは特定のインターフェイスを使用して、デバイスから RADIUS サーバーへの接続を確立します。
  - [ルーティング（Routing）]オプションボタンをクリックして、ルーティングテーブルを使用します。
  - [特定のインターフェイス（Specific Interface）] オプションボタンをクリックし、ドロップダウンリストからセキュリティゾーン/インターフェイスグループまたは Management インターフェイス（デフォルト）を選択します。管理インターフェイスを使用する場合は、明確に選択する必要があります。ただし、ルートルックアップを使用する場合は使用できません。他の管理専用インターフェイスをRADIUSソースとして指定することはできません。ループバック インターフェイス グループを選択することもできます。
- [リダイレクトACL（Redirect ACL）]：リストからリダイレクト ACL を選択するか、新しいリダイレクト ACL を追加します。

（注） これは、リダイレクトされるトラフィックを決定するためにデバイスで定義されている ACL の名前です。ここでのリダイレクト ACL の名前は、ISE サーバーの *redirect-acl* の名前と同じである必要があります。ACL オブジェクトを設定する場合は、ISE サーバーと DNS サーバーに [Block（ブロック）] アクションを、残りのサーバーに [許可（Allow）] アクションを必ず選択してください。

関連トピック

RADIUS サーバーグループの追加 （16 ページ）
RADIUS サーバー グループのオプション （16 ページ）

RADIUS サーバー対応メッセージ オーセンティケータの互換性マトリックス

表 *1 : RADIUS* サーバー対応メッセージ オーセンティケータの *Firewall Management Center* および *Firewall Threat Defense* 互換性マトリックス

Firewall Management Center バージョン	Firewall Threat Defense バージョン	NGIPS	FXOS のバージョン	PAM RADIUS のバージョン
7.7	7.7	—	2.17.0	3.0.0

シングルサインオンサーバーの追加

始める前に

SAML アイデンティティ プロバイダーから次のものを取得します。

- アイデンティティ プロバイダー エンティティ ID URL
- サインイン URL
- サインアウト URL
- アイデンティティ プロバイダー証明書と Firewall Management Center Web インターフェイス（**Devices** > **Certificates**）を使用して Firewall Threat Defense で証明書を登録する

詳細については、SAML シングルサインオン認証の設定を参照してください。

手順

ステップ 1 **Objects** > **Object Management** > **AAA Server** > **Single Sign-on Server**を選択します。

ステップ 2 [シングルサインオンサーバーの追加（Add Single Sign-On Server）] をクリックし、次の詳細を入力します。

- [名前（Name）]：SAML シングル サインオン サーバー オブジェクトの名前。
- [アイデンティティ プロバイダー エンティティ ID（Identity Provider Entity ID）]：サービス プロバイダーを一意に識別するために SAML IdP で定義される URL。

  これは、SAML 発行元が要求に応答する方法を記述したメタデータ XML を提供するページの URL です。
- [SSO URL]：SAML アイデンティティ プロバイダー サーバーにサインインするための URL。
- [ログアウトURL（Logout URL）]：SAML アイデンティティ プロバイダー サーバーからサインアウトするための URL。
- [ベースURL（Base URL）]：アイデンティティ プロバイダー認証が完了するとユーザーを Firewall Threat Defense にリダイレクトする URL。これは、Firewall Threat Defense リモートアクセス VPN 用に設定されたアクセスインターフェイスの URL です。
- [アイデンティティプロバイダー証明書（Identity Provider Certificate）]：IdP によって署名されたメッセージを検証するために Firewall Threat Defense に登録される IdP の証明書。

  リストからアイデンティティプロバイダー証明書を選択するか、**[追加（Add）]** をクリックして新しい証明書登録オブジェクトを作成します。

  詳細については、「Firewall Threat Defense 証明書を管理する」を参照してください。

  Microsoft Azure に登録されたすべてのアプリケーション CA 証明書を Firewall Threat Defense のトラストポイントとして登録する必要があります。Microsoft Azure SAML アイデンティティ プロバイダーは、最初のアプリケーション用に Firewall Threat Defense で構成されます。すべての接続プロファイルは、構成された MS Azure SAML アイデンティティプロバイダーにマップされます。MS Azure アプリケーション（デフォルト以外）ごとに、リモートアクセス VPN の接続プロファイル構成で必要なトラストポイント（CA 証明書）を選択できます。

  詳細は、リモートアクセス VPN の AAA 設定を参照してください。
- [サービスプロバイダー証明書（Service Provider Certificate）]：要求に署名し、IdP との信頼の輪を構築するために使用される Firewall Threat Defense 証明書。

  内部 Firewall Threat Defense 証明書を登録していない場合は、[+] をクリックして証明書を追加および登録します。詳細については、「Firewall Threat Defense 証明書を管理する」を参照してください。
- [要求の署名（Request Signature）]：SAML シングルサインオン要求に署名する暗号化アルゴリズムを選択します。

  署名（SHA1、SHA256、SHA384、SHA512）は、最も弱いものから最も強いものの順で一覧表示されます。暗号化を無効にする場合は、[なし（None）] を選択します。

- [要求タイムアウト（Request Timeout）]：ユーザーがシングルサインオン要求を完了するための SAML アサーション有効期間を指定します。SAML IdPには、*NotBefore* と *NotOnOrAfter* の 2 つのタイムアウトがあります。Firewall Threat Defense は、現在の時刻が（下限）*NotBefore*、および（上限） *NotBefore* + タイムアウト と *NotOnOrAfter* のうちの小さいほうの時間範囲内にあるかどうかを検証します。そのため、IdP の *NotOnOrAfter* タイムアウトよりも長いタイムアウトを設定した場合、指定したタイムアウトは無視され、*NotOnOrAfter* タイムアウトが選択されます。指定したタイムアウトと *NotBefore* タイムアウトの合計が *NotOnOrAfter* の時間より短い場合、そのタイムアウトは Firewall Threat Defense のタイムアウトによってオーバーライドされます。

  タイムアウトの範囲は 1 ー 7200 秒で、デフォルトは 300 秒です。

- [内部ネットワークでのみアクセス可能なIdPを有効にする（Enable IdP only accessible on Internal Network）]：SAML IdP が内部ネットワークに存在する場合は、このオプションを選択します。Firewall Threat Defense はゲートウェイとして機能し、匿名の webvpn セッションを使用してユーザーと IdP 間の通信を確立します。

- [ログイン時に IdP の再認証を要求する（Request IdP re-authentication on Login）]：このオプションをオンにすると、以前の IdP セッションが有効であっても、ログインのたびにユーザーが認証されます。

- [オーバーライドを許可する（Allow Overrides）]：このチェックボックスをオンにすると、このシングル サインオン サーバー オブジェクトのオーバーライドが許可されます。

ステップ 3 **[保存（Save）]** をクリックします。

関連トピック

リモートアクセス VPN の AAA 設定

アクセスリスト

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。これらのオブジェクトは、Firewall Threat Defense デバイスの特定の機能（ルートマップなど）を設定するときに使用します。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、アプリケーショングループに基づいて、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 コンテンツテーブルで [**Objects** > **Object Management** > **Access List** > **Extended**] を選択します。

ステップ 2 次のいずれかを実行します。

- [拡張アクセスリストの追加（Add Extended Access List）] をクリックして、新しいオブジェクトを作成します。
- **Edit** (✎) 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 [新しい拡張アクセスリストオブジェクト（New Extended Access List 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。

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

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。ポートグループは選択できません。

  TCP/UDP の場合、送信元フィールドと宛先フィールドの両方を指定するときは、両方で同じプロトコルを使用する必要があることに注意してください。たとえば、UDP 送信元ポートと TCP 宛先ポートを指定することはできません。

- 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) [アプリケーション（Application）] タブをクリックし、ダイレクト インターネット アクセス ポリシー用にグループ化するアプリケーションを選択します。

重要
- クラスタデバイスのアプリケーションを設定することはできません。したがって、このタブはクラスタデバイスには適用されません。
- ポリシーベースルーティングのアプリケーションでのみ拡張 ACL を使用します。動作が不明でサポートされていないため、他のポリシーでは使用しないでください。拡張 ACL でユーザーアイデンティティと SGT を使用するポリシーベースルーティングのレルム/ISE 設定の移行を確認してください。

（注）

- [利用可能なアプリケーション（Available Applications）] リストには、事前定義されたアプリケーションの固定セットが表示されます。アプリケーションは最初のパケット（IP アドレスとポートに解決される FQDN エンドポイント）によってのみ検出できるため、このリストはアクセス コントロール ポリシーで使用できるアプリケーションのサブセットです。アプリケーション定義は、VDB の更新によって更新され、その後の展開中に Firewall Threat Defense にプッシュされます。
- ユーザー定義のカスタムアプリケーションまたはアプリケーションのグループはサポートされていません。
- 現在、Firewall Management Center ではユーザー定義のカスタムアプリケーションまたはアプリケーションのグループはサポートされておらず、事前定義されたアプリケーションリストを変更することもできません。
- [アプリケーションフィルタ（Application Filters）] にあるフィルタオプションを使用して、このリストを絞り込むことができます。

f) [ユーザー（Users）] タブをクリックし、ポリシーベースルーティング（PBR）に分類されるユーザーとユーザーグループのいずれかまたは両方を選択します。

重要
ポリシーベースルーティングのユーザーとユーザーグループのいずれかまたは両方でのみ拡張 ACL を使用します。動作が不明でサポートされていないため、他のポリシーでは使用しないでください。

（注）
- [使用可能なレルム（Available Realms）] リストには、構成された Active Directory/LDAP レルムが表示されます。レルムの作成と管理については、それぞれLDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成するとレルムを管理するを参照してください。

  （注）
  ローカルレルムと Azure AD レルムはサポートされていません。

- [利用可能なユーザー（Available Users）] リストには、選択した AD/LDAP レルムのダウンロードされたユーザーとユーザーグループが表示されます。ユーザーとユーザーグループのいずれかまたは両方をダウンロードするには、**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** に移動し、関連する Active Directory/LDAP レルムに対する [ダウンロード（Download）] をクリックします。

  （注）
  Threat Defense では、最大 512 のユーザーグループと 64,000 のユーザー - IP マッピングをサポートできます。

- ユーザーから IP へのマッピングおよびユーザー グループ メンバーシップ情報は、ユーザーのログインまたはログアウトおよびグループメンバーシップの変更時に更

新され、 から Firewall Threat Defense に Firewall Management Center プッシュされます。

g) [セキュリティグループタグ（Security Group Tag）] タブをクリックし、ダイレクト インターネット アクセス ポリシーに分類する送信元 SGT タグを選択します。

重要
ポリシーベースルーティングの SGT でのみ拡張 ACL を使用します。動作が不明でサポートされていないため、他のポリシーでは使用しないでください。

（注）
- [使用可能なセキュリティグループタグ（Available Security Group Tags）] リストには、構成されたセキュリティグループタグが表示されます。ISE SGT を使用するか、カスタム SGT を作成するかを選択できます。
- ISE SGT を使用するには、[セッションディレクトリのトピック（Session Directory Topic）] およびサブスクライブされた SXP トピックを使用して Firewall Management Center と ISE が統合されていることを確認します。Cisco ISE 統合の詳細については、「Cisco Identity Services Engine (Cisco ISE) アイデンティティソースの構成方法」を参照してください。

  （注）
  サポートされている ISE バージョンは、3.2、3.1、3.0、および 2.7 パッチ 2 以上です。

- カスタム SGT の作成については、セキュリティ グループ タグ オブジェクトの作成（50 ページ）を参照してください。

h) 必要なアプリケーションを選択し、[ルールの追加（Add Rule）] をクリックします。

（注）
- 拡張 ACL オブジェクトで宛先ネットワークとアプリケーションを構成しないでください。
- 各アクセス コントロール エントリで選択されたアプリケーション（ネットワーク サービス オブジェクト）は、ネットワーク サービス グループ（NSG）を形成し、このグループは Firewall Threat Defense で展開されます。NSG は、ダイレクト インターネット アクセスで使用され、選択したアプリケーショングループとの一致に基づいてトラフィックを分類します。

i) [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。

j) 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、[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 （14 ページ）を参照）。

ステップ 5 **[保存（Save）]** をクリックします。

サービスアクセスオブジェクトの設定

サービス アクセス オブジェクトは、Firewall Threat Defense デバイス上のリモートアクセス VPN などのサービスにアクセスするための、トラフィックの一致条件を定義します。このオブジェクトでは、条件は順番に実行される複数のルールとして定義されます。各サービスアクセスルールには、許可または拒否のアクションと、国、地域、またはユーザー定義の地理位置情報オブジェクトなどの一致条件が設定されています。これらのルールは、地理位置情報に基づいてアクセスを管理し、承認されたリージョンからのトラフィックのみが指定したサービスにアクセスできるようにします。トラフィックがどのルールにも一致しない場合は、デフォルトのアクションが適用されます。

始める前に

- 地理位置情報オブジェクトを設定します。詳細については、位置情報 （58 ページ）を参照してください。
- リモートアクセス VPN ポリシーを設定します。詳細については、新しいリモート アクセス VPN ポリシーの作成を参照してください。

手順

ステップ 1 **Objects** > **Object Management** > **Access List** > **Service Access**を選択します。

ステップ 2 [サービス アクセス オブジェクトの追加（Add Service Access Object）] をクリックして、新しいオブジェクトを作成します。

ステップ 3 [サービス アクセス オブジェクトの追加（Add Service Access Object）] ダイアログボックスで、次のパラメータを設定します。

a) [名前（Name）] フィールドにオブジェクトの名前を入力します。

b) [ルールの追加（Add Rule）] をクリックして、このオブジェクトのサービスアクセスルールを作成します。[サービスアクセスルールの追加（Add Service Access Rule）] ダイアログボックスで、次のパラメータを設定します。

1. ドロップダウンリストで [許可（Allow）] または [拒否（Deny）] のアクションを選択します。
2. [利用可能な国（Available Countries）] から、国、地域、またはユーザー定義の地理位置情報オブジェクトを選択し、それらを [選択した地理位置情報（Selected Geolocation）] リストに移動します。
3. [追加（Add）] をクリックします。

サービスアクセスルールを作成すると、シーケンス番号がルールに割り当てられます。この番号がルールの実行順序を決定します。これらのルールの順序は変更できません。

ステップ 4 [デフォルトアクション（Default Action）] ドロップダウンリストから、[すべての国を許可（Allow All Countries）] または [すべての国を拒否（Deny All Countries）] を選択します。

ステップ 5 （任意）[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、[+] をクリックして、デバイスのサービス アクセス オブジェクトのオーバーライドを設定します。

（注）
デバイスまたはドメインのオーバーライドを定義すると、デバイスまたはドメインでこのオブジェクトが設定されるたびに、元のオブジェクトに定義されている値の代わりにオーバーライド値が使用されます。

ステップ 6 （任意）[サービスアクセスオーバーライドの追加（Add Service Access Override）] ダイアログボックスで、次のパラメータを設定します。

a) [ターゲットデバイスとドメイン（Target Devices and Domains）] ドロップダウンリストから、オーバーライドに必要なデバイスまたはドメインを選択します。
b) 既存のルールが必要かどうかを確認します。それ以外の場合は、それらを削除します。
c) [ルールの追加（Add Rule）] をクリックして、このオブジェクトオーバーライドのサービスアクセスルールを作成します。

1. ドロップダウンリストで [許可（Allow）] または [拒否（Deny）] のアクションを選択します。
2. [利用可能な国（Available Countries）] から、国、地域、またはユーザー定義の地理位置情報オブジェクトを選択し、それらを [選択した地理位置情報（Selected Geolocation）] リストに移動します。
3. [追加（Add）] をクリックします。

d) [デフォルトアクション（Default Action）] ドロップダウンリストから、[すべての国を許可（Allow All Countries）] または [すべての国を拒否（Deny All Countries）] を選択します。
e) [追加（Add）] 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

リモートアクセス VPN ポリシーでサービス アクセス オブジェクトを設定します。詳細については、「リモートアクセス VPN のアクセス インターフェイスの設定」を参照してください。

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 コンテンツ テーブルから **Objects** > **Object Management** > **Access List** > **Standard** を選択します。

ステップ 2 次のいずれかを実行します。

- [標準アクセスリストの追加（Add Standard Access List）] をクリックして、新しいオブジェクトを作成します。
- **Edit** (✎) 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 [新しい標準アクセスリストオブジェクト（New Standard Access List 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。

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

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、[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 （14 ページ）を参照）。

ステップ 5 **[保存（Save）]** をクリックします。

アドレス プール

クラスタリング、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 と IPv6 の両方で、IP アドレスプールを設定できます。 個別インターフェイス モードのクラスタリングでは、MAC アドレス プールを設定することもできます。

手順

ステップ 1 **Objects** > **Object Management** > **Address Pools** を選択します。

ステップ 2 [IPv4プール（IPv4 Pools）] をクリックしてから [IPv4プールの追加（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 （12 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（IPv6 Pools）] をクリックしてから [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 （12 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。

ステップ 6 [MACアドレスプール（MAC Address Pool）] をクリックしてから [MACアドレスプールの追加（Add MAC Address Pool）] をクリックし、次のフィールドを設定します。

個別インターフェイスモードのクラスタリングでは、インターフェイスの MAC アドレスプールを設定できます。インターフェイスに MAC アドレスを手動で設定することはあまりありま

せんが、そのような場合には、このプールを使用して各インターフェイスに一義的な MAC アドレスを割り当てます。「MAC アドレスの設定」を参照してください。

- [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。
- [MACアドレス範囲（MAC Address Range）]：プールで使用できる MAC アドレスの範囲を入力します。開始アドレスと終了アドレスの間にダッシュを使用します（例：000C.F142.4CD1-000C.F142.4CD7）。
- [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 （12 ページ）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。

アクセス制御、 QoS、インテリジェント アプリケーションバイパス、復号など、アプリケーションの照合を許可するさまざまなポリシーでカスタム アプリケーション フィルタを選択できます。

- フィルタを作成するには、システム提供のフィルタを使用してアプリケーションを検索し、それらのアプリケーションを選択して、**[ルールに追加（Add to Rule）]**をクリックします。
- フィルタからアプリケーションを削除するには、アプリケーションの横にある削除アイコンをクリックします。
- アプリケーションに関する情報を表示するには、アプリケーションの横にある情報アイコンをクリックします。

アプリケーション特性の詳細については、 アプリケーションルールの条件を参照してください。

ASパス

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。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 コンテンツテーブルで [**Objects** > **Object Management** > **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、[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 （14 ページ）を参照）。

ステップ 6 **[保存（Save）]** をクリックします。

BFD テンプレート

BFD テンプレートは、一連の BFD 間隔値を指定します。BFD テンプレートで指定された BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。また、シングルホップセッションとマルチホップセッションの認証も設定できます。エコーモードはデフォルトで無効になっています。エコーモードはシングルホップでのみ有効にできます。

手順

ステップ 1 **Objects** > **Object Management** > **BFD Template**を選択します。

ステップ 2 [BFDテンプレートの追加（Add BFD Template）] または [編集（Edit）] をクリックします。

（注）
テンプレートを編集している場合、テンプレートの名前とタイプは変更できません。

ステップ 3 [Template] タブで、次の項目を設定します。

- [Template Name]：この BFD テンプレートの名前。テンプレートの残りのパラメータを設定するには、名前を割り当てる必要があります。テンプレート名にスペースを含めることはできず、数字だけの名前も指定できません。
- [タイプ（Type）] : [シングルホップ（Single-Hop）] または [マルチホップ（Multi-Hop）] オプションボタンをクリックします。
- [Enable Echo]：（オプション）シングルホップテンプレートでエコーをイネーブルにします。

エコー機能がネゴシエートされない場合、検出時間を満たすように高いレートで BFD 制御パケットが送信されます。エコー機能がネゴシエートされている場合、BFD制御パケットはより低速のネゴシエートされたレートで送信され、自己転送されるエコーパケットはより高速のレートで送信されます。可能であれば、エコーモードを使用することを推奨します。

ステップ 4 [Interval] タブで、次の項目を設定します。

a) [間隔タイプ（Interval Type）] ドロップダウンリストから、[マイクロ秒（Microseconds）]、または [ミリ秒（Milliseconds）] を選択します。
b) [乗数（Multiplier）] フィールドに、ホールドダウン時間の計算に使用する値を入力します。この値は、BFD ピアからの連続して見逃す必要がある BFD 制御パケットの数を示します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。デフォルトは 3 です。
c) [最小伝送（Minimum Transmit）] フィールドに最小伝送間隔機能の値を入力します。範囲は 50 ～ 999 ミリ秒または 50,000 ～ 999,000 マイクロ秒です。
d) [最小受信（Minimum Receive）] フィールドに最小受信間隔機能の値を入力します。範囲は 50 ～ 999 ミリ秒または 50,000 ～ 999,000 マイクロ秒です。

ステップ 5 [Authentication] タブで、次の項目を設定します。

- [認証タイプ（Authentication Type）]：ドロップダウンリストから、[NONE]、[md5]、[meticulous-sha-1]、[meticulous-md5]、または [sha-1] を選択します。
- [暗号化パスワード（Encrypted Password）]：（任意）認証パスワードの暗号化を有効にします。
- [パスワード（Password）]：認証されているルーティングプロトコルを使用してパケットで送受信される必要がある認証パスワード。有効な値は、1 ～ 29 文字の大文字と小文字の英数字からなる文字列です。ただし、最初の文字は数字にはできず、数字の後に空白を続けることはできません。たとえば、「1password」や「0 password」は無効です。
- [Key ID]：キー値と照合する共有キー ID。指定できる範囲は 0 ～ 255 です。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックして、BFD テンプレート コンフィギュレーションを保存します。

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

手順

ステップ 1 オブジェクトタイプのリストで、[**Objects** > **Object Management** > **Cipher Suite List**] を選択します。

ステップ 2 [暗号スイートの追加（Add Cipher Suites）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [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 5 [追加（Add）] をクリックします。

ステップ 6 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**Delete** ( )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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

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と照合します。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 コンテンツテーブルで **[Objects > Object Management > 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、[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 （14 ページ）を参照）。

ステップ 9 **[保存（Save）]** をクリックします。

拡張コミュニティ

拡張コミュニティは、共通するいくつかの属性を共有する宛先の大規模なグループです。BGP 拡張コミュニティリストには、共通の属性を共有する一連のプレフィックスをマークするために使用できる属性があります。それらのマーカーは、仮想ルータ間のルートリークを実装するルートをフィルタ処理するために、ルートマップの match 句で使用されます。フィルタリング用の拡張コミュニティリストを使用してポリシーリストオブジェクトを定義することもできます。拡張コミュニティリストは、一致ステートメントの順序付きリストです。ルートは、指定されたルートターゲット（標準）または正規表現（拡張）と一致するものが見つかるまで、ルールと照合されます。[拡張コミュニティ（Extended Community）] ページを使用して、拡張コミュニティ リスト ポリシー オブジェクトを作成および編集します。

（注） 拡張コミュニティリストは、ルートのインポートまたはエクスポートの設定にのみ適用されます。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 [**Objects** > **Object Management** > **Community List** > **Extended Community**] を選択します。

ステップ 2 [拡張コミュニティリストの追加（Add Extended Community List）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、拡張コミュニティ リスト オブジェクトの名前を指定します。名前の長さは 80 文字を超えることはできません。

ステップ 4 拡張コミュニティルールタイプを選択します。

- 1 つ以上のルートターゲットを指定するには、[標準（Standard）] オプションボタンをクリックします。
- 正規表現を指定するには、[拡張（Expanded）] オプションボタンをクリックします。

（注）
同じ拡張コミュニティ リスト オブジェクトに、[標準（Standard）] および [拡張（Expanded）] 拡張コミュニティルールタイプを使用するエントリを含めることはできません。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 拡張コミュニティルールタイプとして [標準（Standard）] を選択した場合は、次の内容を指定します。

a) [シーケンス番号（Sequence No）] フィールドに、ルールを実行する順序を入力します。

シーケンス番号は、リスト内で一意である必要があります。

b) ここで指定したルートターゲットと一致するルートを許可する場合は、[アクション（Action）] ドロップダウンリストから [許可（Allow）] を選択します。ここで指定したルートターゲットと一致するルートを拒否する場合は、[ブロック（Block）] を選択します。

c) [ルートターゲット（Route Target）] フィールドで、ルートターゲットを指定します。

- 1つのエントリに、単一のルートターゲットまたはカンマで区切った一連のルートターゲットを追加できます。例：1:2,1:4,1:6。
- 有効な値は 1:1 ～ 65534:65535 です。
- 1 つのエントリに最大 8 つのルートターゲットを設定できます。
- 複数のエントリに冗長なルートターゲットセットを設定することはできません。たとえば、seq1 に 1:200,100:100,1:300 のルートターゲットを設定し、seq2 に

1:300,100:100,1:200 のルートターゲットを設定するとします。この結果、冗長なルートターゲットセットになり、展開できません。

ステップ 7 拡張コミュニティルールタイプとして [拡張（Expanded）] を選択した場合は、次の内容を指定します。

a) [シーケンス番号（Sequence No）] フィールドに、ルールを実行する順序を入力します。

シーケンス番号は、リスト内で一意である必要があります。

b) ここで指定した正規表現と一致するルートを許可する場合は、[アクション（Action）] ドロップダウンリストから [許可（Allow）] を選択します。ここで指定した正規表現と一致するルートを拒否する場合は、[ブロック（Block）] を選択します。

c) [表現（Expressions）] フィールドで、正規表現を指定します。

- 1 つのエントリに、単一のルートターゲット、またはスペースで区切った一連のルートターゲットを追加できます。例：^((16) | (18)):(.)$。
- エントリには最大 16 の正規表現を追加できます。
- 複数のエントリに冗長な正規表現セットを設定することはできません。たとえば、seq1 に ^((16) | (18)):(.)$ ^4_[0-9]*$ のルートターゲットを設定し、seq2 に ^4_[0-9]*$ ^((16) | (18)):(.)$ のルートターゲットを設定するとします。この結果、冗長な正規表現セットになり、展開できません。

BGP 正規表現の詳細については、こちらを参照してください。

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、[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 （14 ページ）を参照）。

ステップ 9 [保存（Save）] をクリックします。

拡張コミュニティリストは、ルートマップオブジェクトまたはポリシーリストオブジェクトの match 句で参照できます。

- ルートマップオブジェクトでは、拡張コミュニティリストの名前は **[ルートマップエントリの追加（Add Route Map Entry）] > [Match句（Match Clause）] > [BGP] > [コミュニティリスト（Community List）] > [拡張コミュニティリストの追加（Add Extended Community List）]** ダイアログに表示されます。ルートマップでの BGP 設定の設定の詳細については、ルート マップ （93 ページ）を参照してください。
- ポリシーリストオブジェクトでは、拡張コミュニティリストの名前は、**[ポリシーリストの追加（Add Policy List）] > [コミュニティルール（Community Rule）] > [拡張コミュニティリストの追加（Add Extended Community List）]** ダイアログに表示されます。ポリシーリストでの BGP 設定の設定の詳細については、ポリシー リスト （87 ページ）を参照してください。

DHCP IPv6 プール

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature (IPv6 プレフィックス委任クライアントの有効化), you can configure the Firewall Threat Defense to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the Firewall Threat Defense by defining a DHCP IPv6 Pool and assigning it to the DHCPv6 server. The Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. You will configure the client to generate its own IPv6 address by enabling IPv6 autoconfiguration on the client. Enabling stateless autoconfiguration on a client configures IPv6 addresses based on prefixes received in Router Advertisement messages; in other words, based on the prefix that the Firewall Threat Defense received using Prefix Delegation.

プールを追加するには、DHCP IPv6 プールの作成を参照してください。

識別名

それぞれの識別名オブジェクトは、公開キー証明書のサブジェクトまたは発行元に識別名を表します。TLS/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ー証明書を使ってクライアントとサーバーが TLS/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。

（識別名グループは、既存の識別名オブジェクトの名前付きコレクションです。）

識別名は、国コード、共通名、組織、および組織単位で構成できますが、通常は共通名のみで構成されます。たとえば、`https://www.cisco.com` の証明書の共通名は `cisco.com` です。（ただし、必ずしも単純な名前とは限りません。共通名を見つける方法については、識別名（DN）ルールの条件を参照してください）。証明書には、ルール条件で DN として使用できる、複数のサブジェクト代替名（SAN）を含めることができます。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。

共通名を参照する識別名オブジェクトの形式は、`CN=`*name* です。`CN=` なしで DN ルール条件を追加すると、オブジェクトを保存する前に `CN=` が追加されます。

識別名（DN）ルールの条件で詳しく説明されているように、可能な場合は常に Server Name Indication（SNI）を使用して TLS/SSL ルール内の DN が照合されます。

さらに、次の表に示す各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 *2*: 識別名の属性

属性	説明	使用可能な値
C	国番号	2 つの英字
CN	共通名	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

属性	説明	使用可能な値
O	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
OU	組織単位	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

DN ルール条件に関する重要な注意事項

- システムが新しいサーバーへの暗号化セッションを最初に検出したときは、DN データを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。

  サーバーで TLS 1.3 が要求される場合、TLS サーバーアイデンティティ検出を設定すると、decryption policyの判断が行われる前にサーバー証明書が既知の証明書であることを確認するのに役立ちます。詳細については、TLS サーバーアイデンティティ検出を参照してください。

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

ワイルドカードの例

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でのみ一致しますが、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 *3:* 共通名属性のワイルドカードの例

属性	一致する	一致しない
CN=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com

属性	一致する	一致しない
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

（注） DN オブジェクト `CN=amp.cisco.com` は、`CN=auth.amp.cisco.com` のような CN とは一致しないため、このような場合にワイルドカードを推奨します。

詳細および例については、識別名（DN）ルールの条件を参照してください。

関連トピック

識別名（DN）ルールの条件

識別名オブジェクトの作成

手順

ステップ 1 **Objects** > **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。

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 （39 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

DNS サーバ グループ

ドメイン ネーム システム（DNS）サーバーは、www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決します。

DNS サーバー グループ オブジェクトの作成

手順

ステップ 1 ネットワーク オブジェクト リストで [**Objects** > **Object Management** > **DNS Server Group**] を選択します。

ステップ 2 [DNS サーバ グループの追加（Add DNS Server Group）] をクリックします。

ステップ 3 [名前（Name）]を入力します。

ステップ 4 状況に応じて、完全修飾されていないホスト名に追加するために使用される [デフォルト ドメイン（Default Domain）] を入力します。

この設定は、デフォルトのサーバーグループにのみ使用されます。

ステップ 5 デフォルトの [タイムアウト（Timeout）] と [再試行（Retries）] の値は事前入力されています。必要に応じて、これらの値を変更します。

- [再試行（Retries）]：システムが応答を受信しない場合に DNS サーバのリストを再試行する回数（0 ～ 10）。デフォルトは 2 です。
- [タイムアウト（Timeout）]：次の DNS サーバを試行する前に待機する秒数（1 ～ 30）。デフォルト値は 2 秒です。システムがサーバのリストを再試行するたびに、このタイムアウトは 2 倍に増えます。

ステップ 6 このグループの一部になる [DNS サーバ（DNS Servers）] を、IPv4 または IPv6 の形式のカンマ区切りのエントリとして入力します。

1 つのグループには、最大で 6 DNS サーバを含めることができます。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

DNS サーバ グループに設定されている DNS サーバは、DNS プラットフォーム設定でインターフェイス オブジェクトに割り当てる必要があります。詳細については、「DNS」を参照してください。

外部属性

動的オブジェクト

ダイナミックオブジェクトは、REST API コールを使用するか、クラウドソースから IP アドレスを更新できる Dynamic Attributes Connector を使用して取得した 1 つまたは複数の IP アドレスを指定するオブジェクトです。これらのダイナミック オブジェクトは、オブジェクトへの動的な変更を展開しなくても、アクセス制御ルールで使用できます。

（注） 他のほとんどのオブジェクトとは異なり、ダイナミックオブジェクトを有効にするために管理対象デバイスに展開する必要はありません。ダイナミックオブジェクトをルールの**[ダイナミック属性（Dyamic Attributes）]**に追加し、ルールをデプロイします。オブジェクト値は、Dynamic Attributes Connector がプッシュしたらすぐに管理対象デバイスで自動更新されます。

ダイナミックオブジェクトには以下の種類があります。

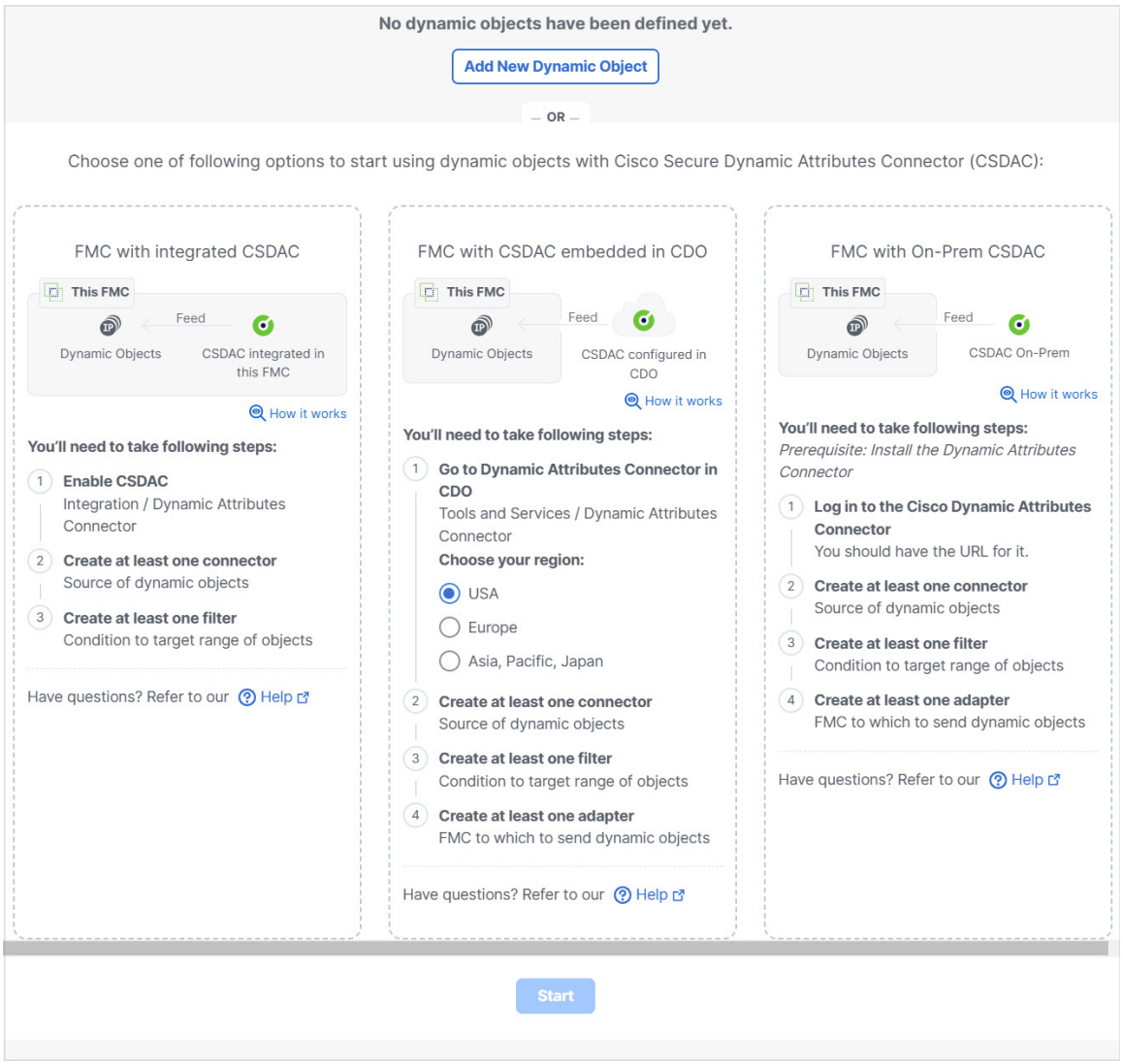
- dynamic attributes connector を使用して作成したダイナミックオブジェクトは、作成されるとすぐに Firewall Management Center にプッシュされ、定期的に更新されます。
- API によって作成されたダイナミックオブジェクト：
  - Classless Inter-Domain Routing（CIDR）の有無にかかわらず、ネットワークオブジェクト同様にアクセスコントロールルールで使用できる IP アドレス。
  - 完全修飾ドメイン名またはアドレス範囲をサポートしていません。
  - API を使用して更新する必要があります。

API によって作成されたダイナミックオブジェクトの詳細については、API で作成したダイナミックオブジェクトについて （49 ページ） を参照してください。

初めてのダイナミックオブジェクトの作成

ダイナミックオブジェクトをまだ設定していない場合は、**Objects** > **Object Management** > **External Attributes** > **Dynamic Object** にあるページが次のように表示されます。

すでにダイナミックオブジェクトを作成している場合は、ダイナミックオブジェクトの処理（48 ページ） を参照してください。



このページを使用するには、次の手順を実行します。

- dynamic attributes connector を展開する方法を表すセクションをクリックします。
- [仕組み（How it works）] をクリックすると図が表示され、そのタイプの展開に関する詳細情報が表示されます。

  詳細については、次の項を参照してください。

  - 組み込みの Dynamic Attributes Connector を使用したダイナミックオブジェクトの作成（45 ページ）
  - Security Cloud Control を使用した動的オブジェクトの作成 （46 ページ）
  - オンプレミス Dynamic Attributes Connector を使用したダイナミックオブジェクトの作成 （47 ページ）

- [開始（Start）] をクリックして、次の関連するアプリケーションを開きます。
  - [統合CSDACを使用したFMC（FMC with Integrated CSDAC）] の方法をクリックした場合、[開始（Start）] をクリックすると **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** に移動し、Dynamic Attributes Connector を有効にして設定できます。

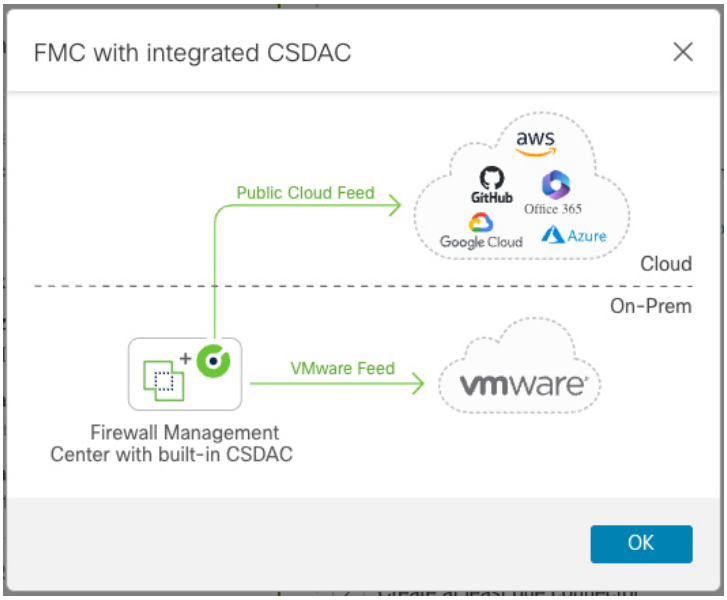
    詳細については、「dynamic attributes connector の有効化」を参照してください。
  - [Security Cloud Controlメソッドに組み込まれたCSDACを使用したFMC（FMC with CSDAC embedded in method）] の方法をクリックした場合、[開始（Start）] をクリックすると Security Cloud Control が開始されます。

    詳細については、『*Security Cloud Control のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理*』というタイトルのガイドを参照してください。
  - [オンプレミスCSDACを使用したFMC] の方法をクリックした場合、[開始（Start）] をクリックすると、まだダウンロードしていない場合は Dynamic Attributes Connector をダウンロードできます。

    詳細については、「*Cisco Secure Dynamic Attributes Connector Configuration Guide*」を参照してください。

組み込みの Dynamic Attributes Connector を使用したダイナミックオブジェクトの作成

この Secure Firewall Management Center で提供される Dynamic Attributes Connector を設定していることを示すと、次のページが表示されます。この Secure Firewall Management Center にはすでに Dynamic Attributes Connector が統合されています（**Integration** > **Dynamic Attributes Connector**）。



このタイプの展開を使用するには、以下の手順を実行します。

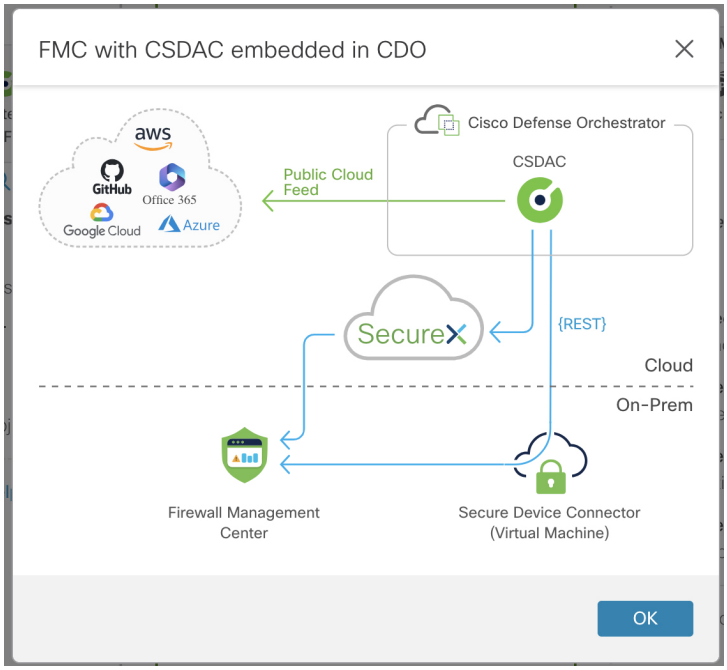
1. Dynamic Attributes Connectorを有効にする（dynamic attributes connector の有効化を参照）
2. クラウドサービスから IP アドレスを取得するコネクタを設定します。

   詳細については、「コネクタを作成する」を参照してください。
3. 動的属性フィルタを設定して、Management Center に送信する IP アドレスを決定します。

   詳細については、「ダイナミック属性フィルタを作成する」を参照してください。
4. **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** でダイナミックオブジェクトを表示します。
5. アクセス制御ルールでダイナミックオブジェクトを使用します（**Policies** > **Access Control heading** > **Access Control** を選択し、[動的属性（Dynamic Attributes）] タブをクリック）。

Security Cloud Control を使用した動的オブジェクトの作成

Security Cloud Control で提供される Dynamic Attributes Connector を設定していることを示すと、次のページが表示されます。



前の図には、Security Cloud Control の設定に関する詳細が記載されていますが、このガイドでは説明していません。詳細については、「Secure Device Connector（SDC）」または「SecureX および Security Cloud Control」を参照してください。

このタイプの展開を使用するには、以下の手順を実行します。

1. クラウドサービスから IP アドレスを取得するコネクタを設定します。

   詳細については、「コネクタを作成する」を参照してください。

2. 動的属性フィルタを設定して、Management Center に送信する IP アドレスを決定します。

   詳細については、「ダイナミック属性フィルタを作成する」を参照してください。

3. Secure Firewall Management Center または Cloud-Delivered Firewall Management Center に IP アドレスを送信するアダプタを設定します。

   詳細は、*Cisco Security Cloud Control: Cloud-Delivered Firewall Management Center for Firewall Threat Defense* でアダプタを作成するセクションを参照してください。

4. アダプタとして定義した Secure Firewall Management Center にログインします。

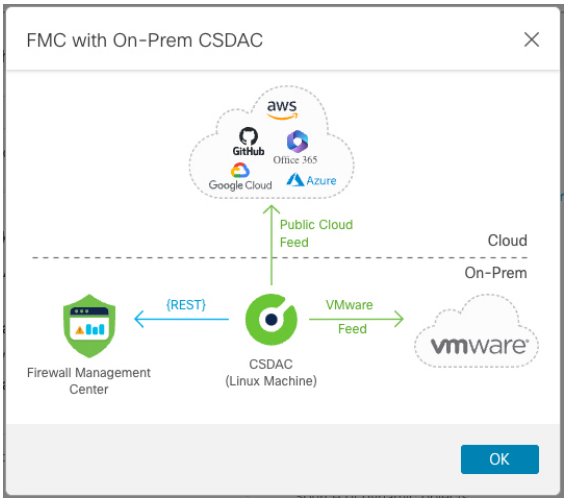
   Secure Firewall Management Center が Security Cloud Control によって管理されている場合は、**[クラウド提供型FMC（Cloud-Delivered FMC）]** をクリックします。

5. **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** でダイナミックオブジェクトを表示します。

6. アクセス制御ルールでダイナミックオブジェクトを使用します（**Policies** > **Access Control heading** > **Access Control** を選択し、[動的属性（Dynamic Attributes）] タブをクリック）。

オンプレミス Dynamic Attributes Connector を使用したダイナミックオブジェクトの作成

以下のページは、ダイナミックオブジェクトを Secure Firewall Management Center または Cloud-Delivered Firewall Management Centerに送信するようにオンプレミス Dynamic Attributes Connector を設定していることを示した場合に表示されます。



このタイプの展開を使用するには、以下の手順を実行します。

1. サポートされている Linux 仮想マシンに Dynamic Attributes Connector をインストールします。

2. クラウドサービスから IP アドレスを取得するコネクタを設定します。

   詳細は、*Cisco Secure Dynamic Attributes Connector Configuration Guide* でコネクタを作成するセクションを参照してください。

3. Secure Firewall Management Center または Cloud-Delivered Firewall Management Center に IP アドレスを送信するアダプタを設定します。

   詳細は、*Cisco Secure Dynamic Attributes Connector Configuration Guide* でアダプタを作成するセクションを参照してください。

4. 動的属性フィルタを設定して、Management Center に送信する IP アドレスを決定します。

   詳細については、*Cisco Secure Dynamic Attributes Connector Configuration Guide* で動的属性フィルタの設定に関するセクションを参照してください。

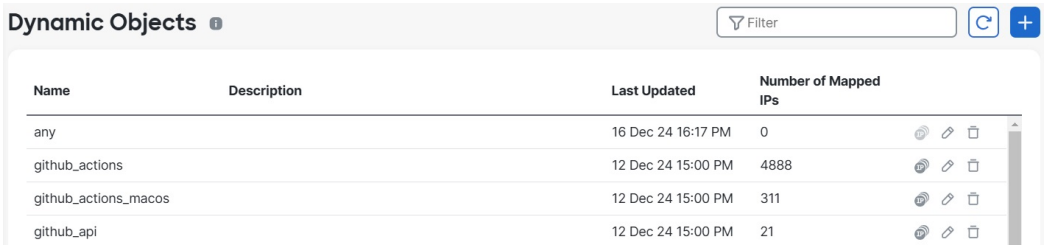
5. **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** でダイナミックオブジェクトを表示します。

6. アクセス制御ルールでダイナミックオブジェクトを使用します（**Policies** > **Access Control heading** > **Access Control** を選択し、[動的属性（Dynamic Attributes）] タブをクリック）。

詳細については、「*Cisco Secure Dynamic Attributes Connector Configuration Guide*」を参照してください。

ダイナミックオブジェクトの処理

すでにいくつかのダイナミックオブジェクトを設定している場合は、**Objects** > **Object Management** > **External Attributes** > **Dynamic Object** にあるページが次のように表示されます。

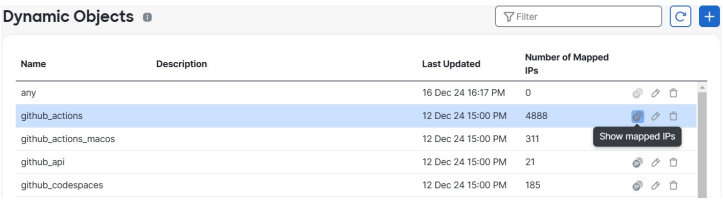


このページには、各ダイナミック オブジェクトに関する情報が表示され、そのオブジェクトに関連付けられている IP アドレスを表示またはダウンロードできます。詳細については、「ダイナミック オブジェクト マッピング （48 ページ）」を参照してください。

ダイナミック オブジェクト マッピング

API または dynamic attributes connector を使用してダイナミックオブジェクトを設定した場合、コネクタは、ダイナミック属性フィルタに一致する IP を定期的に Firewall Management Center に送信します。

これらの IP アドレスの現在のリストを表示またはダウンロードするには、次の図に示すように、[マッピングされたIDの表示（Show Mapped IDs）] をクリックします。



IP アドレスは時間の経過とともに動的に追加されるため、特にアクセスコントロールルールが予期どおりに動作しない場合は、これを定期的に行うことを検討する必要があります。

関連項目

- API で作成したダイナミックオブジェクトについて （49 ページ）
- Dynamic Attributes Connector について

API で作成したダイナミックオブジェクトについて

ダイナミックオブジェクトは、REST API コールを使用するか、クラウドソースから IP アドレスを更新できる Dynamic Attributes Connector を使用して取得した 1 つまたは複数の IP アドレスを指定するオブジェクトです。これらのダイナミック オブジェクトは、オブジェクトへの動的な変更を展開しなくても、アクセス制御ルールで使用できます。

dynamic attributes connector の詳細については、『*Cisco Secure Dynamic Attributes Configuration Guide*』（ガイドへのリンク）を参照してください。https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/200/cisco-secure-dynamic-attributes-connector-v200.html

ダイナミックオブジェクトとネットワークオブジェクトの違いは次のとおりです。

- dynamic attributes connector を使用して作成したダイナミックオブジェクトは、作成されるとすぐに Firewall Management Center にプッシュされ、定期的に更新されます。
- API によって作成されたダイナミックオブジェクト：
  - Classless Inter-Domain Routing（CIDR）の有無にかかわらず、ネットワークオブジェクト同様にアクセスコントロールルールで使用できる IP アドレス。
  - 完全修飾ドメイン名またはアドレス範囲をサポートしていません。
  - API を使用して更新する必要があります。

関連トピック

API で作成したダイナミックオブジェクトの追加または編集 （49 ページ）

API で作成したダイナミックオブジェクトの追加または編集

この手順では、動的オブジェクトを追加または編集する方法について説明します。動的オブジェクトは、Classless Inter-Domain Routing（CIDR）の有無にかかわらず、ネットワークオブジェクトと同様にアクセス制御ルールで使用できる、API を使用する IP アドレスのグループです。

（注） Dynamic Attributes Connector を使用する場合は、動的オブジェクトが自動的に作成されるため、この手順は不要です。

始める前に

オブジェクトサービス REST API を使用して IP オブジェクトにアドレスを入力する方法については、『*Firepower Management Center REST API Quick Start Guide*』を参照してください。動的オブジェクトを展開する必要はありません。

手順

ステップ 1 **Objects** > **Object Management** をクリックします。

ステップ 2 **[External Attributes]** > **[Dynamic Objects]** をクリックします。

ステップ 3 [Add Dynamic Object] または **Edit** (✎) をクリックします。

ステップ 4 オブジェクトの [Name] を入力し、任意で [Description] を入力します。

ステップ 5 [Type] リストで [IP] をクリックします。

次のタスク

必要に応じて、API を使用して動的オブジェクトを更新します。展開する必要はありません。

セキュリティグループタグ

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

これらのオブジェクトは、グローバルドメインでのみ作成できます。これらのオブジェクトを従来型デバイスで使用するには、制御ライセンスが必要です。スマートライセンスデバイスの場合は、どのライセンスでも使用できます。

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。

  Integration > **Other Integrations** > **Identity Sources** をクリックし、**[なし（None）]** をクリックします。そして **[保存（Save）]** をクリックします。

- アイデンティティ ソースの使用のガイドラインについては、ISE/ISE-PIC のガイドラインと制限事項 を参照してください。

手順

ステップ 1 **Objects** > **Object Management** をクリックします。

ステップ 2 **[外部属性（External Attributes）]** > **[セキュリティグループタグ（Security Group Tag）]** をクリックします。

ステップ 3 [Add Security Group Tag] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

ファイル リスト

マルウェア防御 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。

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。Firewall 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。説明にカ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

この手順を実行するには、Malware Defense ライセンスが必要です。

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。

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 **Objects** > **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**Edit** ( )をクリックします。

代わりに **View** ( ) 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

（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

この手順を実行するには、Malware Defense ライセンスが必要です。

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 Secure Firewall 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。

手順

ステップ 1 **Objects** > **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**Edit** ( )をクリックします。

代わりに **View** ( ) 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、[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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

（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

この手順を実行するには、Malware Defense ライセンスが必要です。

手順

ステップ 1 **Objects** > **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**Edit**()をクリックします。

代わりに **View** () 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、[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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

（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

この手順を実行するには、Malware Defense ライセンスが必要です。

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。

手順

ステップ 1 **Objects** > **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 **Edit** (✎) をクリックします。

代わりに **View** (👁) 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 **Edit** (✎) 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 **Delete** (🗑) 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

（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 リストからソース ファイルをダウンロードする

この手順を実行するには、Malware Defense ライセンスが必要です。

手順

ステップ 1 **Objects** > **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 **Edit** (✎) をクリックします。

代わりに **View** (👁) 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 **View** (👁) 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。

FlexConfig

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 Secure Firewall Management Center を使用して設定できない Firewall 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 Firewall 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。Secure Firewall 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。

位置情報

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、リモートアクセス VPN、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

手順

ステップ 1 **Objects** > **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。

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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

インターフェイス（Interface）

各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てることができます。その上で、ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、「内部」インターフェイスを「内部」ゾーンに割り当て、「外部」インターフェイスを「外部」ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、外部から内部に向けては設定できません。ポリシーによっては、セキュリティゾーンだけをサポートする場合も、ゾーンとグループの両方をサポートする場合もあります。

インターフェイス オブジェクトの詳細については、セキュリティ ゾーンとインターフェイス グループを参照してください。

インターフェイス オブジェクトの追加方法については、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を参照してください。

Key Chain

デバイスのデータ セキュリティと保護を向上させるため、IGP ピアを認証するために 180 日以下の期間の循環キーが展開されています。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キーチェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。循環キーは OSPFv2 プロトコルにのみ適用されます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

（注） 認証に使用されるのは MD5 暗号化アルゴリズムのみです。

キーのライフタイム

安定した通信を維持するためには、各デバイスがキー チェーンの認証キーを保存し、複数のキーを同時に機能に使用します。キーの送信と受け入れのライフタイムに基づき、キーのロールオーバーを処理するセキュアなメカニズムがキーチェーン管理によって提供されます。デバイスは、キーのライフタイムを使用してキーチェーン内でアクティブになっているキーを判断します。

キー チェーン内の各キーには 2 つのライフタイムがあります。

- 受け入れライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
- 送信ライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイム中、デバイスはルーティング アップデート パケットをキーとともに送信します。送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

ライフタイムが設定されていない場合は、タイムラインなしで MD5 認証を設定するのと同じことになります。

キーの選択

- キー チェンに複数の有効なキーがある場合、OSPF はライフタイムが最大のキーを選択します。
- ライフタイムが無限のキーが優先されます。
- ライフタイムが同じキーが複数ある場合は、もっとも大きなキー ID を持つキーが優先されます。

キー チェーンのオブジェクトの作成

手順

ステップ 1 **Objects** > **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 [キー チェーン（Key Chain）] を選択します。

ステップ 3 [キー チェーンの追加（Add Key Chain）] をクリックします。

ステップ 4 [キー チェーン オブジェクトの追加（Add Key Chain Object）] ダイアログボックスで、キー チェーンの名前を [名前（Name）] フィールドに入力します。

名前はアンダースコアまたはアルファベットから開始し、英数字文字または特殊文字（-、_、+、 .）を続けます。

ステップ 5 キーをキー チェーンに追加するには、[追加（Add）] をクリックします。

ステップ 6 [キー ID（Key ID）] フィールドにキー識別子を指定します。

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

ステップ 7 [アルゴリズム（Algorithm）] フィールドと [暗号化タイプ（Crypto Encryption Type）] フィールドにサポート対象のアルゴリズムと暗号化タイプ、つまり [MD5] と [プレーン テキスト（Plain Text）] がそれぞれ表示されます。

ステップ 8 [暗号キー文字列（Crypto Key String）] フィールドにパスワードを入力し、[暗号キー文字列の確認（Confirm Crypto Key String）] フィールドにパスワードを再入力します。

- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

ステップ 9 デバイスが他のデバイスとキー交換をしている間にキーを受領/送信する時間間隔をデバイスに設定するには、[受け入れライフタイム（Accept Lifetime）] フィールドと [送信ライフタイム（Send Lifetime）] フィールドにライフタイムの値を指定します。

（注）
デフォルトでは、日時の値は UTC タイムゾーンになります。

終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無期限です。デフォルトの終了時刻は、DateTime です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、それぞれの終了時刻よりも前である必要があります。

ステップ 10 [追加（Add）] をクリックします。

ステップ 5 ～ 10 を繰り返してキーを作成します。キー チェーンにはライフタイムが重複するキーを 2 つ以上作成します。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。

ステップ 11 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、[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 （14 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、[Override] セクションを展開し、[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 （14 ページ）を参照）。

ステップ 12 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

ネットワーク

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は、アクセス コントロール ポリシー、ネットワーク変数、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、ID ポリシーなど、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
```

範囲

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
```

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
```

（注） セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。

[FQDN]

単独の完全修飾ドメイン名（FQDN）FQDN 解決を IPv4 アドレスのみ、IPv6 アドレスのみ、または IPv4 と IPv6 アドレスの両方に制限できます。FQDN は、数字または文字で始まって終わる必要があります。FQDN で内部文字として使用できるのは、文字、数字、およびハイフンだけです。

次に例を示します。

```
www.example.com
```

（注） FQDN オブジェクトは、アクセスコントロールルールとプレフィルタルールまたは手動 NAT ルールのみで使用できます。ルールは、DNS ルックアップを介して FQDN で取得された IP アドレスを一致させます。FQDN ネットワーク オブジェクトを使用するには、DNS サーバー設定を DNS サーバ グループ （42 ページ） で設定し、DNS プラットフォーム設定を DNS で設定していることを確認します。

アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

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。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。

（注） 最大 100 個のネットワークリテラルをネットワークオブジェクトに追加できます。さらに、ネストされた各ネットワーク オブジェクト グループには、最大 100 個のネットワークリテラルを含めることができます。

ネットワーク ワイルドカード マスク

Objects > **Object Management** ページで、ワイルドカード マスク オブジェクトを作成および管理できます。

拡張サブネット IP アドレスを持つネットワークオブジェクトを作成できます。既存のネットワークオブジェクトは、ネットワークオブジェクトとネットワーク ワイルドカード オブジェクトの両方をサポートするように拡張されています。ワイルドカードマスクを使用するネットワークオブジェクトは、ネットワーク オブジェクト リスト ページの [タイプ（Type）] 列に [ネットワークワイルドカード（Network Wildcard）] としてリストされます。

ワイルドカードマスクは、ビットの不連続なマスクである IP アドレスです。連続したマスクを使用して標準ネットワークオブジェクトを作成し、不連続のマスクを使用してワイルドカード ネットワーク オブジェクトを作成できます。

IP アドレスの例	ネットワークワイルドカード ?	オブジェクト タイプ
192.0.0.0/8	なし	ネットワーク
10.10.0.0/255.255.0.0	なし	ネットワーク
10.10.0.10/255.255.0.255	対応	ネットワークワイルドカード
72.0.240.10/255.255.240.255	対応	ネットワークワイルドカード

（注） ネットワーク ワイルドカード オブジェクトと、ネットワーク ワイルドカード オブジェクトを含むオブジェクトグループは、次のポリシーを設定している場合にのみ許可されます。

- プレフィルタ ポリシー
- アクセス コントロール ポリシー
- NAT ポリシー

注意事項と制約事項

- ネットワーク ワイルドカード オブジェクトを作成するには、 Firewall Management Center UI で、**Objects** > **Object Management** > **Network** を選択して **[ネットワークの追加（Add Network）]** をクリックし、**[オブジェクトの追加（Add Object）]** をクリックします。[ネットワーク（Network）] オプションを選択し、拡張サブネットマスクの値を入力します。例：10.0.10.10/255.255.0.255
- オブジェクトのオーバーライド、グループオブジェクトのサポート、グループオブジェクトのオーバーライド、ワイルドカードリテラル、およびワイルドカードオブジェクトのインポートがサポートされています。
- ネットワーク ワイルドカード オブジェクトは、IPv4 アドレスに対してのみサポートされます。
- ネットワーク ワイルドカード オブジェクトは、Firewall Management Center および Firewall Threat Defense 7.1 バージョン以降でサポートされます。
- ネットワーク ワイルドカード オブジェクトは、Snort-3 でのみサポートされます。

ネットワーク オブジェクトの作成

手順

ステップ 1 **Objects** > **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 または、既存のネットワークオブジェクトのクローンを作成し、パラメータを編集して新しいネットワークオブジェクトを作成することもできます。クローンを作成する既存のネットワークオブジェクトの [クローン（Clone）] アイコンをクリックします。

ステップ 5 [Name] を入力します。

ステップ 6 （任意）[Description] に説明を入力します。

ステップ 7 [ネットワーク（Network）] フィールドで、必要なオプションを選択して適切な値を入力します（ネットワーク （62 ページ）を参照）。

（注）
最大100個のネットワークリテラルをネットワークオブジェクトに追加できます。さらに、ネストされた各ネットワーク オブジェクト グループには、最大 100 個のネットワークリテラルを含めることができます。

ステップ 8 （FQDN オブジェクトのみ）[ルックアップ（Lookup）] ドロップダウン メニューから DNS 解決を選択して、IPv4、IPv6、または IPv4 と IPv6 の両方のアドレスを FQDN に関連付けるかを決定します。

ステップ 9 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、[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 （14 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、[Override] セクションを展開し、[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 （14 ページ）を参照）。

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

ネットワークオブジェクトのインポート

ネットワークオブジェクトのインポートの詳細については、オブジェクトのインポート （5 ページ）を参照してください。

PKI

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、サーバー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） Firewall 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ー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。変更を有効にするには、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。

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 証明書および秘密キーのインポート

手順

ステップ 1 **Objects** > **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。

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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

新しい CA 証明書と秘密キーの生成

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。

手順

ステップ 1 **Objects** > **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。

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

手順

ステップ 1 **Objects** > **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。
ステップ 5 ID 属性を入力します。
ステップ 6 [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（70 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

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 **Objects** > **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 **Edit** (✎) をクリックします。
ステップ 4 [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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

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 証明書および秘密キーのダウンロード

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 **Objects** > **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 **Edit** (✎) をクリックします。

ステップ 4 [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。

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。変更を有効にするには、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。

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

手順

ステップ 1 **Objects** > **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。

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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

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

（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 **Objects** > **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 **Edit** (✎) をクリックします。

代わりに **View** (👁) 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

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

手順

ステップ 1 **Objects** > **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。

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 サーバー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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

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。変更を有効にするには、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。

内部証明書オブジェクトの追加

手順

ステップ 1 **Objects** > **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。

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 サーバー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、SCEP、EST、および PKCS12 ファイル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操作は必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。
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、**Objects** > **Object Management** > **PKI** > **Certificate Enrollment** に移動します。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が [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。
  - [EST]：Enrollment over Secure Transport 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によって使用されます。
  - **[SCEP]**：（デフォルト）Simple Certificate Enrollment Protocol（SCEP）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 接続をサポートしている 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（PFX または P12）ファイルとは、サーバ証明書、中間証明書、秘密キーのすべてを暗号化して保持するファイルです。復号のための [パスフレーズ（Passphrase）] 値を入力します。

- [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 （12 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。失敗した登録オブジェクトを編集できます。

- 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）] をクリックして、[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 （78 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
EST 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 ファイルを使用した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

これらのオブジェクトは Firewall Threat Defense デバイスで使用できます。このタスクを実行するには、管理者権限またはネットワーク管理者権限が必要です。

手順

ステップ 1 **[証明書の登録を追加（Add Certificate Enrollment）]** ダイアログを開きます。

- オブジェクト管理から直接：**Objects** > **Object Management** > **PKI** > **Certificate Enrollment** のナビゲーションウィンドウで、**[証明書の登録を追加（Add Certificate Enrollment）]** をクリックします。

- 管理対象デバイスの構成中：**Devices** > **Certificates** 画面で、**[追加（Add）]**、**[新しい証明書を追加（Add New Certificate）]** の順に選択し、**[証明書の登録（Certificate Enrollment）]** フィールドで、[(+)] 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）]** タブをクリックします。

ステップ 4 **[登録の種類（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。

- [EST]：Enrollment over Secure Transport プロトコル。EST 情報を指定します。「証明書の登録オブジェクト EST オプション （81 ページ）」を参照してください。
- [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 （82 ページ）を参照してください。
- **[手動（Manual）]**
  - [CAのみ（CA Only）]：選択した CA から CA 証明書のみを作成するには、このチェックボックスをオンにします。この証明書のアイデンティティ証明書は作成されません。

    このチェックボックスをオンにしない場合、CA 証明書は必須ではありません。CA 証明書がなくても CSR を生成し、アイデンティティ証明書を取得することができます。
  - [CA証明書（CA Certificate）]：CA 証明書を PEM 形式でボックスに貼り付けます。CA 証明書は別のデバイスからコピーして取得することもできます。

    CA 証明書なしで CSR を生成する場合は、このボックスを空のままにできます。
- [PKCS12 ファイル（PKCS12 File）]：VPN 接続をサポートしている Firewall 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、サーバー証明書、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。 Enter the **Passphrase** value for decryption.

ステップ 5 [CA証明書の基本的な制約のCAフラグチェックをスキップする（Skip Check for CA flag in basic constraints of the CA Certificate）]：トラストポイント証明書の基本制約の拡張と CA フラグのチェックをスキップする場合は、このチェックボックスをオンにします。

ステップ 6 [検証用法（Validation Usage）]：VPN 接続中に証明書を検証するオプションから選択します。

- [IPsecクライアント（IPsec Client）]：サイト間 VPN 接続の IPSec クライアント証明書を検証します。
- [SSLクライアント（SSL Client）]：リモートアクセス VPN 接続の試行中に SSL クライアント証明書を検証します。
- [SSLサーバー（SSL Server）]：Cisco Umbrella サーバー証明書など、SSL サーバー証明書を検証する場合に選択します。

ステップ 7 （任意）**[Certificate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 （83 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 8 （任意）**[キー（Key）]** タブをクリックし、キー情報を指定します。証明書の登録オブジェクト の主要なオプション （84 ページ）を参照してください。

ステップ 9 （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 （86 ページ） を参照してください。

ステップ 10 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。

オーバーライドを許可するようにPKCS12証明書の登録オブジェクトを変更するたびに、オーバーライドされるデバイスで証明書の [パスフレーズ（Passphrase）] を更新する必要があります。

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 （12 ページ） を参照してください。

ステップ 11 [保存（Save）] をクリックします。

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
EST 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 ファイルを使用した証明書のインストール

証明書の登録の追加

手順

ステップ 1 [名前（Name）] を入力します。

ステップ 2 [IdP証明書（IdP Certificate）] フィールドに証明書情報を PEM 形式で貼り付けます。

（注）
この証明書がルート証明書または中間証明書に依存している場合は、依存する証明書をインストールする必要があります。「証明書」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。

証明書の登録オブジェクト EST オプション

Secure Firewall Management Center ナビゲーション パス

Objects > **Object Management** > **PKI** > **Certificate Enrollment**。**[証明書の登録を追加（Add Cert Enrollment）]** をクリックして、**[証明書の登録を追加（Add Cert 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

[Enrollment Type]：[EST] に設定します。

（注）
- EST 登録タイプは、EdDSA キーをサポートしていません。
- 証明書の有効期限が切れたときにデバイスを自動登録する EST の機能はサポートされていません。

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

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

[Username]：CA サーバーにアクセスするためのユーザー名。

[Password / Confirm Password]：CA サーバーにアクセスするためのパスワード。

[Fingerprint]：EST を使用して CA 証明書を取得する場合、CA サーバー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。サーバーに直接接続して、CA のフィンガープリントを取得します。

[Source Interface]：CA サーバーと通信するインターフェイス。デフォルトでは、診断インターフェイスが表示されます。データインターフェイスを送信元インターフェイスとして設定するには、各インターフェイスのセキュリティゾーンまたはインターフェイス グループ オブジェクトを選択します。

[Ignore EST Server Certificate Validations]：EST サーバー証明書の検証はデフォルトで実行されます。Firewall Threat Defense による EST サーバー証明書の検証を無視する場合は、このチェックボックスをオンにします。

証明書の登録オブジェクト SCEP オプション

Secure Firewall Management Center ナビゲーション パス

Objects > Object Management > PKI > Certificate Enrollment。**[証明書の登録を追加（Add Cert Enrollment）]** をクリックして、**[証明書の登録を追加（Add Cert 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。

（注） SCEP サーバがホスト名/FQDN で参照されている場合は、FlexConfig オブジェクトを使用して DNS サーバを設定します。

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。サーバー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。

Secure Firewall Management Center ナビゲーション パス

Objects > **Object Management** > **PKI** > **Certificate Enrollment**を確認してください。**[証明書の登録を追加（Add Certificate Enrollment）]** をクリックして、**[証明書の登録を追加（Add Certificate Enrollment）]** ダイアログボックスを開き、**[証明書パラメータ（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

Secure Firewall Management Center ナビゲーション パス

Objects > Object Management > PKI > Certificate Enrollment、**[証明書の登録を追加（Add Certificate Enrollment）]** をクリックして、**[証明書の登録を追加（Add Certificate Enrollment）]** ダイアログボックスを開き、**[キー（Key）]** タブを選択します。

フィールド

- キータイプ：RSA、ECDSA、EdDSA。

（注）
- EST 登録タイプの場合、EdDSA キーはサポートされないため、選択しないでください。
- EdDSA は、サイト間 VPN トポロジでのみサポートされます。
- EdDSA は、リモートアクセス VPN のアイデンティティ証明書としてサポートされていません。

- [Key Name]：証明書に関連付けるキーペアがすでに存在する場合、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、このフィールドでは、登録

時に生成されるキーペアに割り当てる名前を指定します。名前を指定しない場合、完全修飾ドメイン名（FQDN）キーペア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 2048 ビットです。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。

重要

- Firewall Management Center と Firewall Threat Defense のバージョン 7.0 以降では、RSA キーサイズが 2,048 ビット未満の証明書と、SHA-1 と RSA 暗号化アルゴリズムを使用するキーは登録できません。ただし、Weak-Crypto を使用した証明書の PKI 登録を使用すると、SHA-1 と RSA 暗号化アルゴリズムおよび小さなキーサイズを使用する証明書を許可できます。Weak-Crypto を使用した証明書の PKI 登録 （85 ページ）
- Firewall Threat Defense 7.0 では、Weak-Crypto オプションを有効にしても、2048 ビット未満のサイズの RSA キーを生成できません。

- [Advanced Settings]：IPsec リモートクライアント証明書のキーの使用状況エクステンションおよび拡張キーの使用状況エクステンションの値を検証しない場合は、[Ignore IPsec Key Usage] を選択します。IPsec クライアント証明書のキーの使用状況チェックを行わないようにできます。デフォルトでは、このオプションは無効になっています。

（注） サイト間 VPN 接続では、Windows 認証局（CA）を使用する場合、デフォルトのアプリケーション ポリシー拡張は **IP セキュリティ IKE 中間**です。このデフォルト設定を使用している場合は、選択したオブジェクトで [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）] オプションを選択する必要があります。それ以外の場合、エンドポイントはサイト間 VPN 接続を完了できません。

Weak-Crypto を使用した証明書の PKI 登録

SHA-1 ハッシュ署名アルゴリズム、および証明書の 2048 ビット未満の RSA キーサイズは、Firewall Management Center および Firewall Threat Defense バージョン 7.0 以降ではサポートされていません。RSA キーサイズが 2048 ビット未満の証明書は登録できません。

7.0 より前のバージョンを実行している場合、Firewall Management Center を管理する Firewall Threat Defense 7.0 でこれらの制限をオーバーライドするには、Firewall Threat Defense で Enable Weak-Crypto オプションを使用できます。Weak-Crypto キーを許可することは推奨しません。このようなキーは、キーサイズが大きいキーほど安全ではないためです。

（注） Firewall Threat Defense 7.0 以降では、Weak-Crypto を許可している場合でも、2048 ビット未満のサイズの RSA キーの生成はサポートされません。

デバイスで Weak-Crypto を有効にするには、**Devices** > **Certificates** ページに移動します。Firewall Threat Defense デバイスに対して表示される **Enable Weak-Crypto**( )ボタンをクリックします。Weak-Crypto オプションを有効にすると、ボタンが に変わります。デフォルトでは、Weak-Crypto オプションは無効になっています。

（注） 弱い暗号の使用が原因で証明書の登録が失敗した場合、Firewall Management Center は Weak-Crypto オプションを有効にするように求める警告メッセージを表示します。同様に、[Enable Weak-Crypto] ボタンをオンにすると、Firewall Management Center はデバイスで Weak-Crypto の設定を有効にする前に警告メッセージを表示します。

Firewall Threat Defense の旧バージョンから 7.0 へのアップグレード

Firewall Threat Defense 7.0 にアップグレードする場合、既存の証明書の設定は保持されます。ただし、これらの証明書に 2048 ビット未満の RSA キーがあり、SHA-1 暗号化アルゴリズムを使用している場合は、それらを使用して VPN 接続を確立することはできません。2048 ビットより大きい RSA キーサイズの証明書を購入するか、または VPN 接続の Permit Weak-Crypto オプションを有効にする必要があります。

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。

Secure Firewall Management Center ナビゲーション パス

Objects > **Object Management** > **PKI** > **Certificate Enrollment**、( )**[証明書の登録を追加（Add Cert Enrollment）]** をクリックし、**[証明書の登録を追加（Add Cert 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。

URL は、**http://** で始まる必要があります。URL にポート番号を含めてください。IPv6 アドレスは、角カッコで囲みます（例：*http://[0:0:0:0:0.18:0a01:7c16]*）。

- [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。

  URL は、**http://** で始まる必要があります。IPv6 アドレスは、角カッコで囲みます（例：*http://[0:0:0:0:0.18:0a01:7c16]*）。

- [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 cannot 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。

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 リストを設定できる。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。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 **Objects** > **Object Management** > **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）] リストに、デバイスが管理ステーションとの通信を行うインターフェイスが含まれた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）] タブをクリックして、BGP コミュニティまたは拡張コミュニティを、指定されたコミュニティ リスト オブジェクトまたは拡張コミュニティ リスト オブジェクトとそれぞれ照合できるようにします。複数のルールを指定すると、一致する許可または拒否が満たされるまで、ルートがルールに対して検証されます。

a) ルールに対してコミュニティリストを指定するには、[選択したコミュニティリスト（Selected Community List）] フィールドで [既定（given）] をクリックします。**Edit** (✎)コミュニティリストが [使用可能なコミュニティリスト（Available Community List）] の下に表示されます。必要なリストを選択して [追加（Add）] をクリックし、[OK] をクリックします。

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。

b) 拡張コミュニティリストを追加するには、[選択した拡張コミュニティリスト（Selected Extended Community List）] フィールドで [既定（given）] をクリックします。**Edit** (✎)拡張コミュニティリストが [使用可能な拡張コミュニティリスト（Available Extended Community

List）] の下に表示されます。必要なリストを選択して [追加（Add）] をクリックし、[OK] をクリックします。

（注）
拡張コミュニティリストは、ルートのインポートまたはエクスポートの設定にのみ適用されます。

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、[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 （14 ページ）を参照）。

ステップ 13 **[保存（Save）]** をクリックします。

ポート

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。

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

手順

ステップ 1 **Objects** > **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。

または、既存のポートオブジェクトのクローンを作成し、パラメータを編集して新しいポート オブジェクトを作成することもできます。クローンを作成する既存のポートオブジェクトの [クローン（Clone）] アイコンをクリックします。

ステップ 4 名前を入力します。

ステップ 5 [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、[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 （14 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、[Override] セクションを展開し、[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 （14 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

ポートオブジェクトのインポート

ポートオブジェクトのインポートの詳細については、オブジェクトのインポート （5 ページ）を参照してください。

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。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 コンテンツ テーブルから **Objects** > **Object Management** > **Prefix Lists** > **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、[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 （14 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。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 コンテンツ テーブルから **Objects** > **Object Management** > **Prefix Lists** > **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、[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 （14 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。

このオブジェクトは Firewall Threat Defense デバイスで使用できます。

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

- 拡張コミュニティリストを追加します。

（注） 拡張コミュニティリストは、ルートのインポートまたはエクスポートの設定にのみ適用されます。

- ポリシー リストの追加

手順

ステップ 1 **Objects** > **Object Management** > **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が生じた場合の番号の間隔を確保するために、少なくとも 10 間隔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）]：（入力/出力）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. [コミュニティリスト（Community List）] タブをクリックして、BGP コミュニティまたは拡張コミュニティを、指定されたコミュニティ リスト オブジェクトまたは拡張コミュニティ リスト オブジェクトとそれぞれ照合できるようにします。
   - ルールに対してコミュニティリストを指定するには、[選択したコミュニティリスト（Selected Community List）] フィールドで [既定（given）] をクリックします。**Edit** (✎)コミュニティリストが [使用可能なコミュニティリスト（Available Community List）] の下に表示されます。必要なリストを選択して [追加（Add）] をクリックし、[OK] をクリックします。コミュニティ リスト オブジェクトの作成方法については、コミュニティ リスト （35 ページ）を参照してください。
   - 拡張コミュニティリストを追加するには、[選択した拡張コミュニティリスト（Selected Extended Community List）] フィールドで [既定（given）] をクリックします。**Edit** (✎)拡張コミュニティリストが [使用可能な拡張コミュニティリスト（Available Extended Community List）] の下に表示されます。必要なリストを選択して [追加（Add）] をクリックし、[OK] をクリックします。拡張コミュニティ リスト オブジェクトの作成方法については、拡張コミュニティ （36 ページ）を参照してください。

   BGP コミュニティと指定したコミュニティ リスト オブジェクト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。このオプションは、拡張コミュニティリストには適用されません。

   （注）
   複数のルールを指定すると、一致する許可または拒否条件が満たされるまで、ルートがルールに対して検証されます。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。

- [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。

   [特定のコミュニティ（Specific Community）] の下で、次の手順を実行します。

   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。

   [特定の拡張コミュニティ（Specific Extended Community）] の [ルーターゲット（Route Target）] フィールドに、ルーターゲット番号を ASN:nn 形式で入力します。

   - 1:1 ー 65534:65535 の範囲の値を入力できます。

     1 つのエントリに、単一のルーターゲットまたはカンマで区切った一連のルーターゲットを追加できます。例：1:2,1:4,1:6。

   - 1 つのエントリに最大 8 つのルーターゲットを設定できます。
   - ルートマップ間で冗長ルーターゲットエントリを設定することはできません。

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、任意の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、[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 （14 ページ）を参照）。

ステップ10 **[保存（Save）]**をクリックします。

セキュリティ インテリジェンス

セキュリティ インテリジェンス機能には、IPSライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

セキュリティインテリジェンスのリストとフィードは、リストまたはフィードのエントリに一致するトラフィックをすばやくフィルタリングするために使用できるIPアドレス、ドメイン名、およびURLのコレクションです。

- リストは、手動で管理される静的コレクションです。
- 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。

セキュリティ インテリジェンスのリストとフィードは、次のようにグループ化されます。

- DNS（ドメイン名）
- ネットワーク（IPアドレス）
- URL

システムが提供するフィード

シスコでは、セキュリティインテリジェンスオブジェクトとして次のフィードを提供しています。

- Talosからの最新の脅威インテリジェンスで定期的に更新されるセキュリティインテリジェンスフィード。
  - Cisco-DNS-and-URL-Intelligence-Feed（[DNS Lists and Feeds]の下）
  - Cisco-Intelligence-Feed（IPアドレス用、[Network Lists and Feeds]の下）

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。

- Cisco-TID-Feed（[Network Lists and Feeds] の下）

  このフィードは、アクセス コントロール ポリシーの [Security Intelligence] タブでは使用されません。

  代わりに、Secure Firewall Threat Intelligence Director を有効化および設定して、TID オブザーバブルデータのコレクションであるこのフィードを使用するようする必要があります。

  このオブジェクトを使用して、このデータが TID 要素に公開される頻度を設定します。

  詳細については、Threat Intelligence Directorを参照してください。

事前定義リスト：グローバルブロックリストとグローバルブロックしないリスト

システムには、ドメイン（DNS）、IP アドレス（ネットワーク）、および URL の定義済みグローバルブロックリストとブロックしないリストが付属しています。

これらのリストは、入力するまで空です。これらのリストを作成するには、グローバルおよびドメインのセキュリティインテリジェンスリスト （100 ページ）を参照してください。

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これらのリストを使用します。

カスタムフィード

サードパーティーのフィードやカスタム内部フィードを使用すると、複数の Secure Firewall Management Center アプライアンスからなる大規模な展開で企業全体のブロックリストを簡単に保守できます。

「カスタム セキュリティ インテリジェンス フィード （107 ページ）」を参照してください。

カスタムリスト

カスタム リストを強化し、フィードとグローバル リストを微調整できます。

「カスタム セキュリティ インテリジェンス リスト （109 ページ）」を参照してください。

セキュリティ インテリジェンスのリストとフィードが使われる状況

- IP アドレスとアドレスブロック：セキュリティ インテリジェンスの一部として、アクセス コントロール ポリシーでブロックリストとブロックしないリストを使用します。
- ドメイン名：セキュリティ インテリジェンスの一部として、DNS ポリシーでブロックリストとブロックしないリストを使用します。
- URL：セキュリティ インテリジェンスの一部として、アクセス コントロール ポリシーでブロックリストとブロックしないリストを使用します。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。

セキュリティ インテリジェンス オブジェクトの変更方法

ブロックリスト、ブロックしないリスト、フィード、またはシンクホールオブジェクトのエントリを追加または削除するには：

オブジェクト タイプ	機能の編集	編集後に再度展開しますか?
カスタムのブロックリストとブロックしないリスト	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。	×
デフォルト（カスタム入力）ブロックリストとブロックしないリスト：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するか、オブジェクトマネージャを使用してエントリを削除します。	×
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。	×
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。	×
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。	はい

グローバルおよびドメインのセキュリティインテリジェンスリスト

Firewall Management Center には、グローバルブロックリストとブロックなしリストが含まれています。これらのリストを使用すると、セキュリティインテリジェンスを使用して、特定の接続を一貫してブロックできます。また、特定の接続のブロックを免除して、設定済みの別の脅威検出プロセスによるそれらの接続の評価を可能に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一連の IP アドレスに気付いた場合、それらの IP アドレスを即座にブロ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。

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ロック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ブロックしない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。

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

マルチテナント追加：

- 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ブロックリストまたはブロックしないリスト。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ブロックリストまたはブロックしないリスト。

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。

- ドメインブロックリスト：Company A、ドメインブロックしないリスト：Company A
- DNS のドメインブロックリスト：Company A、DNS のドメインブロックしないリスト：Company A
- URL のドメインブロックリスト：Company A、URL のドメインブロックしないリスト：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ロックリストまたはブロックしない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同じ IP アドレスをグローバルドメインと Company A のブロックリストに追加できますが、Company B のドメインのブロ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）グローバルブロックリスト
- （Company A の管理者のみが削除できる）ドメインブロックリスト- Company A

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ブロックしないリストまたはブロックリストです。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ーは独自の展開で項目をブロックリストやブロックしない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。

- 子孫ブロックリスト - Global、子孫のブロックしないリスト - Global
- DNS の子孫ブロックリスト - Global、子孫の DNS のブロックしないリスト - Global
- URL の子孫ブロックリスト - Global、子孫の URL のブロックしないリスト - Global

（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。

グローバル セキュリティ インテリジェンス リストへのエントリの追加

イベントとダッシュボードを確認するときに、事前定義されたブロックリストに追加することで、それらのイベント内の IP アドレス、ドメイン、および URL を含む将来のトラフィックを即座にブロックできます。

同様に、セキュリティインテリジェンスのブロック後に脅威検出プロセスで評価する必要があるトラフィックをセキュリティインテリジェンスがブロックしている場合は、イベントからの IP アドレス、ドメイン、および URL を事前定義された「ブロックしない」リストに追加できます。

脅威検出のセキュリティ インテリジェンス フェーズで、これらのリストのエントリに照らしてトラフィックが評価されます。

これらリストの詳細については、グローバルおよびドメインのセキュリティインテリジェンス リスト （100 ページ） を参照してください。

始める前に

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、次のユーザーロールのうち 1 つが必須です。

- 管理者
- 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。

必要に応じて、これらのリストが予定通りのポリシー内で使用されていることを確認してください。

手順

ステップ 1 セキュリティ インテリジェンスを使用して常にブロックするか、セキュリティ インテリジェンスのブロックから除外する IP アドレス、ドメイン、または URL を含むイベントに移動します。

ステップ 2 IP アドレス、ドメイン、または URL を右クリックし、適切なオプションを選択します。

項目タイプ	コンテキスト メニュー オプション
IP アドレス	ブロックリストに IP を追加 ブロックしないリストに IP を追加 これらのオプションは、ネットワークのそれぞれのリストに IP アドレスを追加します。
URL	URL のグローバルブロックリストに URL を追加 URL のグローバルブロックしないリストに URL を追加
URL フィールドの URL ドメイン	URL のグローバルブロックリストにドメインを追加 URL のグローバルブロックしないリストにドメインを追加
DNS クエリフィールドのドメイン	DNS のグローバルブロックリストにドメインを追加 DNS のグローバルブロックしないリストにドメインを追加

次のタスク

これらの変更を有効にするために再展開する必要はありません。

リストから項目を削除する方法は、グローバル セキュリティ インテリジェンス リストからのエントリを削除する （103 ページ） を参照してください。

グローバル セキュリティ インテリジェンス リストからのエントリを削除する

（注） これらのリストにエントリを追加するにはグローバル セキュリティ インテリジェンス リストへのエントリの追加 （102 ページ） を参照してください。

手順

ステップ 1 **Objects** > **Object Management** > **Security Intelligence**を選択します。

ステップ 2 適切なオプションをクリックします。

- [ネットワークのリストとフィード（Network Lists and Feeds）]（IP アドレス用）
- [DNSのリストとフィード（DNS Lists and Feeds）]（ドメイン名用）
- [URLのリストとフィード（URL Lists and Feeds）]

ステップ 3 グローバルブロックリストまたはグローバルブロックしないリストの横にある鉛筆をクリックします。

ステップ 4 削除するエントリの横にあるごみ箱ボタンをクリックします。

セキュリティ インテリジェンスのリストとフィードの更新

リストとフィードの更新は、既存のリストまたはフィードファイルを新しいファイルの内容に置き換えます。既存ファイルと新しいファイルの内容は結合されていません。

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。

デフォルトでは、各フィードは 2 時間ごとに Management Center を更新します。この頻度は変更できます。Management Center が受信したすべての更新は、すぐに管理対象デバイスに渡されます。また、管理対象デバイスは、変更について 30 分ごとに Firewall Management Center をポーリングします。この周波数を変更することはできません。

フィードの更新間隔を変更するには、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 （104 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 フィードの更新頻度の変更

Firewall Management Center がセキュリティ インテリジェンス フィードを更新する間隔を指定できます。

フィードの更新の詳細については、セキュリティインテリジェンスのリストとフィードの更新（104 ページ）を参照してください。

手順

ステップ 1 **Objects** > **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。

システムが提供する URL フィードは、[DNSリストとフィード（DNS Lists and Feeds）] の下のドメインフィードと結合されます。

ステップ 3 更新するフィードの横にある **Edit** (✎) をクリックします。

代わりに **View** (👁) 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 インテリジェンスのリストとフィード

カスタムリストとカスタムフィード：要件

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。

フィードの要件

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 エンコードすることができません。

フィードの更新間隔が 30 分以下の場合は、MD5 URL を指定する必要があります。これにより、変更されていないフィードの頻繁なダウンロードが防止されます。フィードサーバーが

MD5 URL を提供しない場合は、30 分以上間隔を空けてダウンロードを使用する必要があります。

MD5 チェックサムを使用する場合は、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。

URL リストとフィード：URL 構文と一致基準

セキュリティ インテリジェンスの URL リストとフィード（カスタムのリストとフィード、およびグローバルのブロックリストとブロックしないリストのエントリを含む）には、以下を含めることができます。これらは、説明されている一致の動作を持ちます。

- ホスト名

  たとえば、**www.example.com** などです。

- URL

  example.com は、**example.com** とすべてのサブドメインと一致します（**www.example.com**、**eu.example.com**、**example.com/abc**、および **www.example.com/def** を含む）。ただし、**example.co.uk** または **examplexyz.com** または **example.com.malicious-site.com** とは一致しません

  URL フィードまたはリストに 1 つのエントリが含まれている場合、それらのドメインで終わるすべての URL が識別されてブロックされます。

  例：**www.netflix.com, www.amazon.*、org、edu、www.hulu.*** の URL フィードがグローバルなブロックリストに追加されると、次のコンテンツがブロックされます。http://www.amazon.in、http://www.rajiv.org/、http://www.edu.edu/、http://www.edu.org/、http://org.org/ および http://edu.edu。

  https://www.cisco.com/c/en/us/products/security/firewalls/index.html のように、URL パス全体を含めることもできます

（注） カスタム URL、ネットワーク、および DNS フィードを作成できます。ここでは、URL 自体にユーザー名とパスワードを追加できます（例：**https://admin:password@server.domain.com/list.txt**）。

ただし、パスワードにコロン（:）やアットマーク（@）などの特殊文字が含まれている場合、送信は失敗します。パスワードに特殊文字が含まれていないことを確認してください。または、URL でエンコードされたパスワードを使用することもできます。

- 完全一致を指定するための URL の末尾のスラッシュ

  example.com/ は、**example.com** のみと一致します。**www.example.com** またはその他の URL とは一致しません。

- URL 内の任意のドメインを表すワイルドカード（*）

アスタリスクは、ドットで区切られた完全なドメイン文字列を表すことができますが、ドメイン文字列の一部を表すことはできません。また、最初のスラッシュの後に続く URL の一部を表すことはできません。

有効な例：

- **`*.example.com`**
- **`www.*.com`**
- **`example.*`**

  （これは、**`example.com`**、**`example.org`**、および **`example.de`** などと一致しますが、**`example.co.uk`** とは一致しません）
- **`*.example.*`**
- **`example.*/`**

無効な例：

- **`example*.com`**
- **`example.com/*`**

- IP アドレス（IPv4）

  IPv6 アドレスの場合や、範囲または CIDR 表記を使用する場合は、セキュリティ インテリジェンス ネットワーク オブジェクトを使用します。

  10.10.10.* や 10.10.*.* などの、オクテットを表す 1 つ以上のワイルドカードを含めることができます。

カスタム セキュリティ インテリジェンス リスト （109 ページ） も参照してください。

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ブロックリストおよびブロックしないリストによって、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。内部フィードのセットアップもできます。内部フィードは、1 つのソースリストを使用して導入環境で複数の Secure Firewall Management Center アプライアンス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 ブロックをブロックリストまたはブロックしないリストに追加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ーまたはブロックする場合は、[モニター（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。

MD5 チェックサムを使用して、更新された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は、内部フィードに MD5 チェックサムを使用することをお勧めします。

（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。

システムがインターネットからフィードを更新するタイミングを厳密に制御する場合は、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、自動更新を使用すると、最新の関連データであることが確認されます。

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。

完全な要件については、カスタムリストとカスタムフィード：要件（105 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 フィードの作成

IPSライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **Objects** > **Object Management** > **Security Intelligence** ノードを選択し、追加するフィードタイプを選択します。

ステップ 2 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。

- [ネットワークのリストとフィードの追加（Add Network Lists and Feeds）]（IP アドレス用）
- **[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 3 フィードの名前を [名前（Name）] に入力します。

ステップ 4 [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 5 [フィード URL（Feed URL）] を入力します。

ステップ 6 [MD5 URL] を入力します。

これは、フィードの内容が最後の更新以降に変更されたかどうかを判断するために使用され、システムは変更されていないフィードをダウンロードしません。

30 分より短い更新間隔には MD5 URL が必要です。

フィードサーバーが MD5 URL を提供しない場合は、30 分以上の間隔を選択する必要があります。

ステップ 7 [更新頻度（Update Frequency）] を選択します。

ステップ 8 [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

IPSライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

始める前に

少なくとも 1 つのデバイスが管理センターに追加されている必要があります。

手順

ステップ 1 **Objects** > **Object Management** > **Security Intelligence** を選択します。

ステップ 2 [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 3 [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、Secure Firewall 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 Secure Firewall 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 ポリシーのブロ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ブロックしない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 ブロックをブロックリストまたはブロックしないリストに追加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ーまたはブロックする場合は、[モニター（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。
- 追加のフォーマット要件については、カスタムリストとカスタムフィード：要件（105ページ）を参照してください。

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。

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

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 **Objects** > **Object Management** > **Security Intelligence** ノードを選択し、リストタイプを選択します。

ステップ 2 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。

- [ネットワークのリストとフィードの追加（Add Network Lists and Feeds）]（IP アドレス用）
- **[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 3 名前を入力します。

ステップ 4 [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 5 [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 6 [保存（Save）] をクリックします。

次のタスク

これらの変更を有効にするために再展開する必要はありません。リストからエントリを削除する方法は、グローバル セキュリティ インテリジェンス リストからのエントリを削除する （103 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 リストの更新

手順

ステップ 1 **Objects** > **Object Management** > **Security Intelligence** ノードを選択し、リストタイプを選択します。

ステップ 2 更新するリストの横にある**Edit** ( )をクリックします。

代わりに **View** ( ) 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 3 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 4 必要に応じてリストを変更します。

ステップ 5 [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 6 [保存（Save）] をクリックします。

次のタスク

これらの変更を有効にするために再展開する必要はありません。リストからエントリを削除する方法は、グローバル セキュリティ インテリジェンス リストからのエントリを削除する （103 ページ） を参照してください。

シンクホール

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、またはサーバーに解決されない IP アドレスのいずれかを付与する DNS サーバーを

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

IPSライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **Objects** > **Object Management** > **Sinkhole** を選択します。

ステップ 2 [Add Sinkhole] をクリックします。

ステップ 3 [Name] を入力します。

ステップ 4 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 5 次の選択肢があります。

- シンクホール サーバーへのトラフィックをリダイレクトする場合は、[Log Connections to Sinkhole] を選択します。
- トラフィックを非解決 IP アドレスにリダイレクトするには、[Block and Log Connections to Sinkhole] を選択します。

ステップ 6 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 7 **[保存（Save）]** をクリックします。

SLA モニタ

各インターネット プロトコル サービス レベル契約（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 モニター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）。インターネット プロトコル サービス レベル契約（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 モニターを使用することはできません.

これらのオブジェクトは Firewall Threat Defense デバイスで使用できます。

手順

ステップ 1 **Objects** > **Object Management** > **SLA Monitor** を選択します。

ステップ 2 [SLA モニターの追加（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、Secure Firewall 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ーされている IP アドレスを入力します。

ステップ 13 [使用可能なゾーン（Available Zones）] リストには、ゾーンとインターフェイス グループの両方が表示されます。[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またはインターフェイス グループを追加します。1つのインターフェイスを指定するには、インターフェイスにゾーンまたはインターフェイスのグループを作成する必要があります。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を参照してください。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。

時間範囲

時間範囲オブジェクトを使用して、ルールをいつ適用するのかを決定するために使用する期間を定義します。

（注） 時間ベースの ACL は、Firewall Management Center 7.0 以降の Snort 3 でもサポートされています。

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。このオブジェクトはFirewall Threat Defenseデバイスでのみ機能することに注意してください。

時間範囲オブジェクトは、このトピックの最後にリストされているポリシータイプでのみ指定できます。

（注） タイムゾーンはデバイスのローカル時間を表し、時間範囲をサポートするポリシーのルールでその時間範囲を適用するためにのみ使用されます。タイムゾーンによってデバイスの設定された時刻が変更されることはありません。設定を確認するには、Firewall Threat Defense CLI で **show time-range timezone** および **show time** コマンドを使用します（*Cisco Secure Firewall Threat Defense Command Reference* ガイドを参照）。さらに、シャーシのタイムゾーンは管理センターのタイムゾーンに優先します。

始める前に

時間範囲は、トラフィックを処理するデバイスに関連付けられているタイムゾーンに基づいて適用されます。デフォルトでは、これはUTCです。デバイスに関連付けられているタイムゾーンを変更するには、[**Devices** > **Platform Settings**] に移動します。

手順

ステップ 1 オブジェクトタイプのリストで、[**Objects** > **Object Management** > **Time Range**] を選択します。

ステップ 2 [時間範囲の追加（Add Time Range）] をクリックします。

ステップ 3 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。
- [デバイス（Device）] > [プラットフォーム設定（Platform Settings）] でデバイスのタイムゾーンを指定しないかぎり、すべての時間は 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。
- 1 つのオブジェクトで最大 28 の期間を指定できます。
- 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 4 [保存（Save）] をクリックします。

次のタスク

次のいずれかで時間範囲を設定します。

- アクセス コントロール ルール
- プレフィルタ ルール
- トンネル ルール
- VPN グループポリシー

VPN グループ ポリシー オブジェクトでは、[アクセス時間（Access Hours）] フィールドを使用して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 （142 ページ） および グループ ポリシーの詳細オプション （151 ページ） を参照してください。

タイムゾーン

管理対象デバイスのローカルタイムゾーンを指定するには、タイムゾーンオブジェクトを作成し、デバイスに割り当てられたデバイスプラットフォーム設定ポリシーでそのオブジェクトを指定します。

このデバイスのローカルタイムは、アクセス制御、プレフィルタ、VPN グループポリシーなどの、時間範囲をサポートしているポリシーのルールで時間範囲を適用するためにのみ使用されます。デバイスにタイムゾーンを割り当てない場合、これらのポリシーで時間範囲を適用するときは、デフォルトでは UTC が使用されます。システムの他の機能では、タイムゾーンオブジェクトで指定されたタイムゾーンは使用されません。

タイムゾーンオブジェクトは、Firewall Threat Defense デバイスでのみサポートされています。

（注） 時間ベースの ACL は、Firewall Management Center 7.0 以降の Snort 3 でもサポートされています。

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 ゾーンを使用したトンネル レベルでのアクセス制御の適用を参照してください。

URL

重要 セキュリティ インテリジェンス設定、およびアクセス コントロール ポリシーと QoS ポリシーの URL ルールにこのオプションおよび同様のオプションを使用する場合のベストプラクティスについては、手動 URL フィルタリングオプション を参照してください。

URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループ オブジェクトは複数の URL またはアドレスを定義できます。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。

URL オブジェクトを作成する場合は、次の点に注意してください。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。1 つ以上の / を含める場合、文字列の部分一致には URL 文字列全体が使用されます。次に、次のいずれかに該当する場合、URL は一致と見なされます。
  - 文字列が URL の先頭にある。
  - 文字列がドットの後に続く。
  - 文字列の先頭にドットが含まれている。
  - 文字列が :// 文字の後に続く。

  たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。

（注） サーバーは再構成でき、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部（つまり / 文字を含む URL 文字列）をブロックまたは許可するために手動の URL フィルタリングは使用しないことをお勧めします。

- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成するときに、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。
- 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。また、システムはサブジェクト共通名に含まれるサブドメインを無視するので、サブドメイン情報を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。

ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

URL オブジェクトの作成

手順

ステップ 1 オブジェクトタイプのリストで、[**Objects** > **Object Management** > **URL**] を選択します。

ステップ 2 [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 3 [Name] を入力します。

ステップ 4 （任意）[Description] に説明を入力します。

ステップ 5 [URL] に、URL または IP アドレスを入力します。

ステップ 6 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、[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 （14 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、[Override]セクションを展開し、[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 （14 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

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、adaptive profile updates、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。

システム提供の多くの共有オブジェクトルールと標準テキストルールでは、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が定義されます。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、変数がユーザー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 サーバーが含まれていれば、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ーされます。

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。

初めに、定義済みのデフォルト値で構成される単一のデフォルトの変数セットが提供されます。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 Talos Intelligence Group 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。

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 （133 ページ）
変数セットの管理 （132 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。

- ユーザー定義変数

  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。Talos Intelligence Group 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 *4:* 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 Instant Messenger（AIM）サーバを定義し、チャット ベースのルールおよび 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。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバーに特に影響するルールを作成する場合、$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。
$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、暗号化されていないポートを定義します。	不要。
$FTP_PORTS	ネットワーク上の FTP サーバーのポートを定義し、FTP サーバーのエクスプロイト ルールに使用されます。	はい。FTP サーバーがデフォルト 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監視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。

変数名	説明	変更しますか
$HTTP_PORTS	ネットワーク上の Web サーバーのポートを定義し、Web サーバーのエクスプロイト ルールに使用されます。	はい。web サーバーがデフォルト 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。
$SIP_SERVERS	ネットワーク上で SIP サーバを定義し、SIP をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SIP サーバーを実行している場合は、$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	ネットワーク上でデータベース サーバを定義し、データベースをターゲットとしたエクスプロイトを解決するルールで使用されます。	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 サーバーのポートを定義し、SSH サーバーのエクスプロイト ルールに使用されます。	はい。デフォルト ポート以外の SSH サーバー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）。

変数名	説明	変更しますか
$SSH_SERVERS	ネットワーク上でSSHサーバを定義し、SSHをターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SSHサーバーを実行している場合は、$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	ネットワーク上で既知の Telnet サーバを定義し、Telnet サーバをターゲットとしたエクスプロイトを解決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。
$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adaptive profile updates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。
- adaptive profile updates：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、システムで提供されている拡張変数は、USER_CONF 変数のみです。

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。

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 *5:* 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	any
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

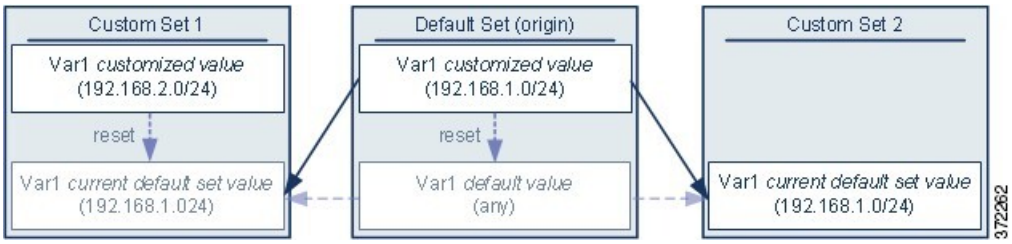
セットに変数を追加する

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。

- **設定値を使用する場合**（たとえば、192.168.0.0/16）、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 セットへのユーザー定義変数の追加

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。



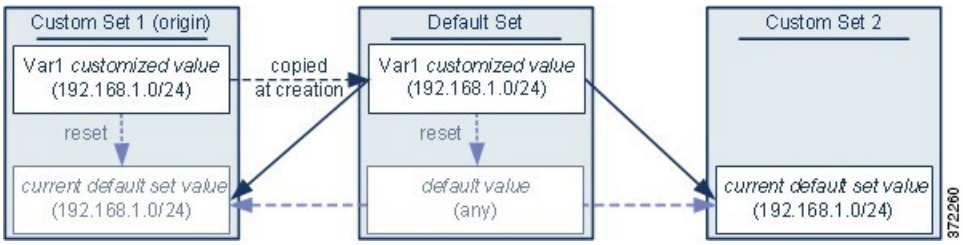
任意のセットで Var1 の値をカスタマイズできます。Var1 がカスタマイズされていない Custom Set 2 では、この値は 192.168.1.0/24 です。Custom Set 1 では、Var1 のカスタマイズ値 192.168.2.0/24 はデフォルト値をオーバーライドします。デフォルト セットのユーザ定義変数をリセットすると、すべてのセットのそのデフォルト値が any にリセットされます。

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、ユーザー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。

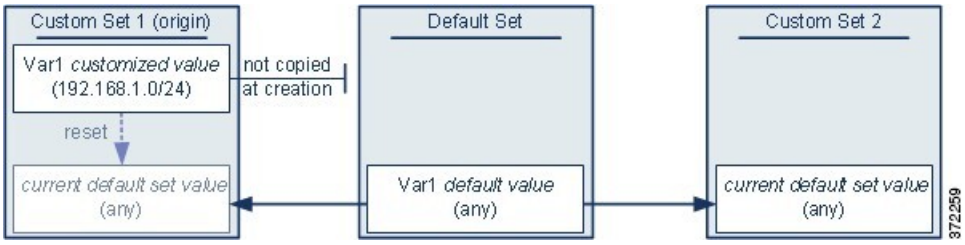
例：カスタム セットへのユーザー定義変数の追加

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	ユーザー定義	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	ユーザー定義	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	ユーザー定義	10.4.0.0/16	—
NOT_DMZ_NET	ユーザー定義	—	DMZ_NET
NONCORE_NET	ユーザー定義	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	ユーザー定義	10.4.0.0/16	—
NONCORE_NET	ユーザー定義	—	HOME_NET DMZ_NET

変数セットの管理

変数セットを使用するには、IPS ライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **Objects** > **Object Management** > **Variable Set**を選択します。

ステップ 2 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 （133 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**Delete** ()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**Edit** ()をクリックします。オブジェクトの編集 （8 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**Clear** ()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 （133 ページ）を参照してください。

変数セットの作成

手順

ステップ 1 **Objects** > **Object Management** > **Variable Set**を選択します。
ステップ 2 [変数セットの追加（Add Variable Set）] をクリックします。
ステップ 3 [Name] を入力します。
ステップ 4 （任意）[Description] に説明を入力します。
ステップ 5 セット内の変数を管理します（変数の管理 （133 ページ）を参照）。
ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

変数の管理

IPSライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

手順

ステップ 1 **Objects** > **Object Management** > **Variable Set** を選択します。
ステップ 2 編集する変数セットの横にある **Edit** () をクリックします。

代わりに **View** () 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 3 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 （134 ページ）を参照してください。
- 削除：変数の横にある **Delete** () 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ー定義変数
- 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 **Edit**(✎)をクリックします。「変数の編集（135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（Reset）]をクリックします。[リセット（Reset）]がグレー表示になっている場合は、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（Reset）]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 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。

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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

変数の追加

IPSライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

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 **Delete** ( ) 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。

- [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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

変数の編集

IPSライセンス（Firewall Threat Defense デバイスの場合）または保護ライセンス（他のすべてのデバイスタイプ）が必要です。

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 **Edit** () をクリックします。

代わりに **View** () 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。
- 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 **Delete** () 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

VLAN タグ

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

手順

ステップ 1 **Objects** > **Object Management** > **VLAN Tag** を選択します。

ステップ 2 [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 3 名前を入力します。

ステップ 4 [説明（Description）] を入力します。

ステップ 5 [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 6 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、[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 （14 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、[Override] セクションを展開し、[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 （14 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

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

VPN

Firewall Threat Defense デバイスでは、次の VPN オブジェクトを使用できます。これらのオブジェクトを使用するには、管理者権限が必要であり、スマート ライセンス アカウントが輸出規制を満たす必要があります。これらのオブジェクトは、リーフドメインでのみ設定できます。

証明書マップオブジェクト

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

Objects > **Object Management** > **VPN** > **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、ユーザー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。
  - [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。
  - [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。

（注） [SER（シリアル番号）コンポーネント（SER (Serial Number) component）]：[サブジェクト（Subject）] フィールドにシリアル番号を指定していることを確認します。証明書マップは、サブジェクト名内のシリアル番号属性とのみ一致します。

  - [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

Secure Client カスタム属性オブジェクト

カスタム属性は、Secure Clientが、Per App VPN、Allow or Defer Upgrade、および Dynamic Split Tunneling などの機能を設定するために使用します。カスタム属性にはタイプと名前付きの値があります。まず属性のタイプを定義した後、このタイプの名前付きの値を 1 つ以上定義できます。Firewall Management Center を使用してセキュアクライアントカスタム属性オブジェクトを作成し、オブジェクトをグループポリシーに追加し、グループポリシーをリモートアクセス VPN に関連付けて、VPN クライアントの機能を有効にすることができます。

Firewall Threat Defense は、カスタム属性オブジェクトを使用して次の機能をサポートします。

- **Per App VPN**：Per App VPN 機能は、アプリを識別し、Firewall Threat Defense 管理者によって許可されたアプリケーションのみを VPN 経由でトンネリングするのに役立ちます。
- **Allow or Defer Upgrade**：Secure Client ユーザーは、遅延アップグレードを使用して、Secure Clientアップグレードのダウンロードを遅らせることができます。クライアントアップデートが使用できる場合、Secure Client で更新するかアップグレードを延期するかを尋ねるダイアログを開くための属性を設定できます。
- **Dynamic Split Tunneling**：Dynamic Split Tunneling を使用すると、VPN トンネルから IP アドレスまたはネットワークを含めたり除外したりするポリシーをプロビジョニングできます。ダイナミック スプリット トンネリングを設定するには、カスタム属性を作成し、グループ ポリシーに追加します。

Secure Client カスタム属性を設定するための段階的な手順については、Secure Clientのカスタム属性オブジェクトの追加 （140 ページ）および次を参照してください：

機能に対して設定する固有のカスタム属性の詳細については、使用している Secure Client リリースの『*Cisco Secure Client (including AnyConnect) Administrator Guide*』を参照してください。

関連トピック

グループポリシーの Secure Clientオプション （146 ページ）

Secure Clientのカスタム属性オブジェクトの追加

始める前に

Per App VPN のカスタム属性オブジェクトを追加する前に、次のことを確認してください。

- Per App VPN が MDM 経由で適切に設定されていて、各デバイスが MDM サーバーに登録されている必要があります。
- Cisco Secure Client企業アプリケーション セレクタ ツールを使用して、アプリケーションごとに Base64 エンコード文字列を作成します。
  1. ここから Cisco Secure Client企業アプリケーション セレクタ ツールをダウンロードします。
  2. アプリケーション選択ツールを開き、左上にあるドロップダウンメニューからモバイルプラットフォームを選択します。
  3. フレンドリ名とアプリケーション ID を入力してルールを追加します。残りのフィールドの指定は任意です。
  4. メニューバーで、[Policy] をクリックします。エンコードされた Base65 ルールは、エンコードされた形式で表示されます。
  5. ポリシー文字列を選択してコピーし、後で Secure Client のカスタム属性オブジェクトを作成するときに使用するために保存します。

手順

ステップ 1 **Objects** > **Object Management** > **VPN** > **Custom Attribute**を選択します。

ステップ 2 **[Secure Clientカスタム属性の追加（Add Secure Client Custom Attribute）]** をクリックします。

ステップ 3 [Name] を入力し、任意で属性の [Description] を入力します。

ステップ 4 **[Secure Client属性（Secure Client Attribute）]** ドロップダウンリストから属性を選択します。

- [Per App VPN]：このオプションを選択し、[Attribute Value] ボックスに Base64 エンコード文字列を指定します。
- [延期更新を許可（Allow Defer Update）]：次のオプションのいずれかを選択し、Secure Clientの更新を許可または延期するために必要な情報を指定します。
  - [Show the prompt until user takes action]：VPN クライアントの更新を許可するか延期するかを選択するまで、VPN ユーザーにプロンプトを表示します。
  - [Show the prompt until times out]：指定した期間にプロンプトを表示し、[Timeout] ボックスで期間を指定するには、このオプションを選択します。
  - [Do not show the prompt and take automatic action]：VPN の更新を自動的に許可または延期するには、このオプションを選択します。

- [Default Action]：ユーザーが応答しない場合、またはユーザーが介入しない自動アクションを設定する場合に実行するデフォルトアクションを選択します。Secure Client を更新するか、更新を延期するかを選択できます。
- [最小バージョン（Minimum Version）]：更新を許可または延期するために、クライアントシステムに存在する必要がある最小の Secure Client バージョンを指定します。

- [Dynamic Split Tunneling]：IP アドレスまたはネットワークを VPN トンネルに含めるか、または VPN トンネルから除外するには、このオプションを選択します。
  - [Include domains]：リモートアクセス VPN トンネルに含めるドメイン名を指定します。
  - [Exclude domains]：リモートアクセス VPN トンネルから除外するドメイン名を指定します。

ステップ 5 [Allow Overrides] 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許可します。

ステップ 6 [保存（Save）] をクリックします。
カスタム属性オブジェクトがリストに追加されます。

次のタスク

カスタム属性をグループポリシーに関連付けます。グループポリシーへのカスタム属性の追加（141 ページ）を参照してください。

グループポリシーへのカスタム属性の追加

グループポリシーをリモートアクセス VPN 接続に使用するには、Secure Client カスタム属性をグループポリシーに関連付ける必要があります。を

手順

ステップ 1 **Objects** > **Object Management** > **VPN** > **Group Policy** を選択します。

ステップ 2 新しいグループ ポリシーを追加するか、既存のグループ ポリシーを編集します。

ステップ 3 **[Secure Client]** > **[カスタム属性（Custom Attributes）]** の順にクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[Secure Client属性（Secure Client Attribute）]**（Per App VPN、Allow Defer Update、または Dynamic Split Tunneling）を選択します。

ステップ 6 リストから [Custom Attribute Object] を選択します。

（注）
[追加（Add）]（+）をクリックして、選択した Secure Client 属性の新しいカスタム属性オブジェクトを作成します。**Objects** > **Object Management** > **VPN** > **Custom Attribute** で、カスタム

属性オブジェクトを作成することもできます。「Secure Clientのカスタム属性オブジェクトの追加 （140 ページ）」を参照してください。

ステップ 7 [Add] をクリックして属性をグループポリシーに保存し、[Save] をクリックしてグループポリシーへの変更を保存します。

関連トピック

グループポリシーの Secure Clientオプション （146 ページ）

Firewall 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。

ユーザー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 承認サーバーがグループ 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） Firewall Threat Defense にグループポリシー属性の継承はありません。ユーザーについては、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 サーバー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 ポリシーがユーザーに対して特定されていない場合にのみ使用されます。

グループオブジェクトを使用するには、エクスポート制御機能が有効なスマート ライセンス アカウントに関連付けられている次の Secure Clientライセンスのいずれかが必要です。

- Secure Client VPN Only
- Secure Client Advantage
- Secure Client Premier

関連トピック

グループ ポリシー オブジェクトの設定 （142 ページ）

グループ ポリシー オブジェクトの設定

Firewall Threat Defense グループ ポリシー オブジェクト （142 ページ）を参照してください。

手順

ステップ 1 **Objects** > **Object Management** > **VPN** > **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。ユーザーのアクセス 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 Click **Add Group Policy** or choose a current policy to edit.

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 （143 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 グループポリシーの Secure Clientオプション （146 ページ）の説明に従って、このグループポリシーの **[Secure Client]** 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 （151 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。

グループ ポリシー一般オプション

ナビゲーション パス

Objects > **Object Management** > **VPN** > **Group Policy**、**[グループポリシーを追加する（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、**[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] です。

IP アドレス プール

リモート アクセス VPN のユーザ グループに固有のアドレス プールに基づいて適用される IPv4 アドレス割り当てを指定します。リモート アクセス VPN では、認証に RADIUS/ISE を使用して、識別されたユーザ グループの特定のアドレス プールから IP アドレスを割り当てることが

できます。特定のユーザ グループに対して、特定のグループ ポリシーを RADIUS 認証属性（GroupPolicy/Class）として設定することにより、非アイデンティティアウェア システム内のユーザまたはユーザ グループにポリシーの適用をシームレスに実行できます。たとえば、請負業者用に特定のアドレス プールを選択して、これらのアドレスを使用してポリシーの適用を行い、内部ネットワークへの制限付きのアクセスを許可する必要があります。

Firewall Threat Defense デバイスがクライアントに IPv4 アドレスプールを割り当てる優先順位：

1. IPv4 アドレス プールの RADIUS 属性
2. グループ ポリシーの RADIUS 属性
3. 接続プロファイルにマップされたグループ ポリシー内のアドレス プール
4. 接続プロファイル内の IPv4 アドレス プール

グループ ポリシーで IP アドレス プールを使用する際の制限事項の一部を以下に示します。

- IPv6 アドレス プールはサポートされていません。
- グループ ポリシーでは、最大で 6 つの IPv4 アドレス プールを設定できます。
- 使用中のアドレス プールが変更されると、展開が失敗します。アドレス プールを変更する前に、すべてのユーザをログオフする必要があります。
- アドレス プールの名前が変更されたり、重複するアドレス プールが設定されると、展開が失敗する可能性があります。変更を展開するには、古いアドレス プールを削除してから、変更されたアドレス プールを展開する必要があります。

  トラブルシューティング コマンドの一部を以下に示します。

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

バナー フィールド

ログイン時にユーザー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、Secure Client 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 ユーザー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）サーバーおよび Windows Internet Naming System（WINS）サーバー。Secure Client の名前解決に使用されます。

- [プライマリ DNS サーバー（Primary DNS Server）] および [セカンダリ DNS サーバー（Secondary DNS Server）]：このグループで使用する DNS サーバーの 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 サーバー（Primary WINS Server）] および [セカンダリ WINS サーバー（Secondary WINS Server）]：このグループで使用する WINS サーバーの 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ネットワークスコープ（DHCP Network Scope）]：目的のプールと同じサブネット上にあり、プール内にないルーティング可能な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。DHCP サーバーは、この IP アドレスが属するサブネットを判別し、そのプールからのIPアドレスを割り当てます。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。

  接続プロファイルのアドレスプールにDHCPサーバーを設定した場合、DHCPスコープはこのグループのプールに使用するサブネットを識別します。DHCPサーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用するDHCPサーバーで定義されているアドレスプールのサブセットを選択できます。

  ネットワーク スコープを定義しない場合、DHCPサーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

  ルーティングの目的で可能な場合は常に、インターフェイスの IP アドレスを使用することを推奨します。たとえば、プールが 10.100.10.2 ～ 10.100.10.254 で、インターフェイス アドレスが 10.100.10.1/24 の場合、DHCP スコープとして 10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP は IPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

  LINK-SELECTION（RFC 3527）およびSUBNET-SELECTION（RFC 3011）は現在サポートされていません。
- [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 （22 ページ）を参照してください。

（注） バージョン 7.4 以降、**[標準アクセスリスト（Standard Access List）]** オプションはデフォルトで無効になっています。アクセスリストを追加するには、**[拡張アクセスリスト（Extended Access List）]** オプションを使用します。

- [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 サーバー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、491 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 （142 ページ）

グループポリシーの Secure Clientオプション

以下の仕様は、Secure Client VPN の動作に適用されます。

ナビゲーション

Objects > **Object Management** > **VPN** > **Group Policy**。Click **Add Group Policy** or choose a current policy to edit.次に、**[Secure Client]** 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）]：Secure Client 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、ファイルオブジェクト （158 ページ）を参照してください。

Secure Client 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。Secure Client ソフトウェアは、クライアントのユーザー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 Secure Client機能を有効にする設定も行われます。

Secure Client 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 Secure Client プロファイルエディタ を使用します。詳細については、『Cisco Secure Client (including AnyConnect) Administrator Guide』の該当するリリースの「*Secure Client* プロファイルエディタ」章を参照してください。

管理プロファイルのフィールド

管理 VPN トンネルは、エンドユーザーが VPN 経由で接続していない場合でも、エンドポイントの電源が投入されるたびに企業ネットワークへの接続を提供します。

[Management VPN Profile]：管理プロファイルファイルには、エンドポイントで管理 VPN トンネルを有効にして確立するための設定が含まれています。

スタンドアロン管理 VPN トンネル プロファイル エディタを使用して、新しいプロファイルファイルを作成したり、既存のプロファイルファイルを変更したりできます。プロファイルエディタはシスコのソフトウェア ダウンロード センターからダウンロードできます。

プロファイルファイルの追加に関する詳細については、ファイルオブジェクト （158 ページ）を参照してください。

クライアントモジュールのフィールド

Cisco Secure Client VPN Onlyは、さまざまな組み込みモジュールによって、強化されたセキュリティを提供します。これらのモジュールは、Web セキュリティ、エンドポイントフローに対するネットワークの可視性、オフネットワークローミング保護などのサービスを提供します。各クライアントモジュールには、要件に応じたカスタム設定のグループを含むクライアントプロファイルが含まれています。

次の Secure Client モジュールはオプションであり、VPN ユーザーが Secure Client をダウンロードしたときにダウンロードされるようにこれらのモジュールを設定できます。

- **AMP イネーブラ**：エンドポイント向けの高度なマルウェア防御（AMP）を導入します。
- **DART**：トラブルシューティングのために CiscoTAC に送信できるシステムログおよびその他の診断情報のスナップショットをキャプチャします。
- **ISE ポスチャ**：OPSWAT ライブラリを使用してポスチャチェックを実行し、エンドポイントの適合性を評価します。
- **ネットワーク アクセス マネージャ**：有線とワイヤレスの両方のネットワークにアクセスするための 802.1X（レイヤ 2）とデバイス認証を備えています。
- **ネットワーク可視性**：キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。
- **Start Before Login**：Windows のログインダイアログボックスが表示される前に Secure Client を開始することにより、ユーザーを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。

- **Umbrella Roaming Security**：アクティブな VPN がないときに DNS レイヤセキュリティを提供します。
- **Web セキュリティ**：定義されているセキュリティポリシーに基づいて、Web ページの要素を分析し、許容可能なコンテンツを許可し、悪意のあるコンテンツまたは許容できないコンテンツをブロックします。

[追加（Add）] をクリックし、クライアントモジュールごとに次を選択します。

- [クライアントモジュール（Client Module）]：リストから Secure Clientモジュールを選択します。
- [ダウンロードするプロファイル（Profile to download）]：Secure Client 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、ファイルオブジェクト （158 ページ）を参照してください。
- [モジュールのダウンロードを有効化（Enable module download）]：オンにすると、エンドポイントがプロファイルとともにクライアントモジュールをダウンロードできるようになります。オフの場合、エンドポイントはクライアントプロファイルだけをダウンロードできます。

各モジュールのクライアントプロファイルを作成するには、独立した設定ツールである GUI ベースの Secure Client プロファイルエディタ を使用します。Secure Client プロファイルエディタ はシスコのソフトウェア ダウンロード センターからダウンロードしてください。詳細については、『Cisco Secure Client (including AnyConnect)』の該当するリリースの「*Secure Client* 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 Secure Client VPN Onlyによって確立された SSL VPN 接続の最大伝送ユニット（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

- **[Secure Client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 Secure 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 on ...）]** . 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。

  Secure Client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 Secure Client 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 Secure Client 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。

カスタム属性フィールド

ここでは、Secure Client が、アプリごとの VPN、アップグレードの許可または延期、およびダイナミック スプリット トンネリングなどの機能を設定するために使用する Secure Client カスタム属性を示します。[Add] をクリックして、カスタム属性をグループポリシーに追加します。

1. [Secure Client属性（Secure Client Attribute）]（[アプリごとのVPN（Per App VPN）]、[延期更新を許可（Allow Defer Update）]、または [ダイナミックスプリットトンネリング（Dynamic Split Tunneling）]）を選択します。
2. リストから [Custom Attribute Object] を選択します。

（注） [追加（Add）]（+）をクリックして、選択した Secure Client 属性の新しいカスタム属性オブジェクトを作成します。**Objects** > **Object Management** > **VPN** > **Custom Attribute** で、カスタム属性オブジェクトを作成することもできます。「Secure Clientのカスタム属性オブジェクトの追加 （140 ページ）」を参照してください。

3. [Add] をクリックして属性をグループポリシーに保存し、[Save] をクリックしてグループポリシーへの変更を保存します。

関連トピック

グループ ポリシー オブジェクトの設定 （142 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

Objects > **Object Management** > **VPN** > **Group Policy**。Click **Add Group Policy** or choose a current policy to edit. その後、**[詳細（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、プロトコルなどの条件に基づきます。VPN フィルタは初期接続にのみ適用されます。アプリケーション インスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。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 （114 ページ）を参照してください。
- [ユーザーあたり同時ログイン（Simultaneous Logins Per User）]：ユーザー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、ユーザー 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）]：最大ユーザー接続時間（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ー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）]：このユーザーのアイドル 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ー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 （142 ページ）

Firewall 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の各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

手順

ステップ 1 **Objects** > **Object Management** > **VPN** > **IKEv1 IPsec Proposal** 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 **Edit**（）、**View**（）、または **Delete**（）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。オプションの詳しい説明については、Deciding Which Encryption Algorithm to Use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。

オプションの詳しい説明については、Deciding Which Hash Algorithms to Use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

手順

ステップ 1 コンテンツテーブルで [**Objects** > **Object Management** > **VPN** > **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 **Edit**（）、**View**（）、または **Delete**（）できます。

ステップ 2 **[IKEv2 IPsec プロポーザルを追加（Add IKEv2 IPsec Proposal）]** を選択し、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。

（注）

Firewall Threat Defense は、NULL 暗号化を使用する IPSec トンネルをサポートしていません。IPSec IKEv2 プロポーザルには NULL 暗号化を選択しないでください。

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。 オプションの詳しい説明については、Deciding Which Hash Algorithms to Use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。このプロポーザルに Encapsulating Security Protocol（ESP）暗号化アルゴリズムを使用します。

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。 オプションの詳しい説明については、Deciding Which Encryption Algorithm to Useを参照してください。

ステップ 7 [保存（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。

IKE ポリシー

Internet Key Exchange（IKE; インターネット キー交換）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。。

IKEv1 ポリシー オブジェクトの設定

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 コンテンツテーブルで [**Objects** > **Object Management** > **VPN** > **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 **Edit**（）、**View**（）、または **Delete**（）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。 オプションの詳しい説明については、Deciding Which Encryption Algorithm to Use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。 オプションの詳しい説明については、Deciding Which Hash Algorithms to Use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。 オプションの詳しい説明については、Deciding Which Diffie-Hellman Modulus Group to Use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 サーバー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

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 コンテンツテーブルで [**Objects** > **Object Management** > **VPN** > **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**Edit** ( )、**View** ( )、または**Delete** ( )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。オプションの詳しい説明については、Deciding Which Hash Algorithms to Use 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。 オプションの詳しい説明については、Deciding Which Encryption Algorithm to Use 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 ポリシーに使用されるハッシュ アルゴリズムの疑似乱数関数（PRF）部分です。IKEv1 では、整合性アルゴリズムと PRF アルゴリズムを分けることができません。ただし、IKEv2 で

は、これらのエレメントに対して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。 オプションの詳しい説明については、Deciding Which Hash Algorithms to Useを参照してください。

ステップ 10 暗号化には、**[Diffie-Hellman グループ（Diffie-Hellman Group）]** を選択します。

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。 オプションの詳しい説明については、Deciding Which Diffie-Hellman Modulus Group to Use を参照してください。

ステップ 11 [保存（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。

Secure Client のカスタマイズ

Secure Client をカスタマイズして、それらのカスタマイズを VPN ヘッドエンドに展開できるようになりました。エンドユーザーが Secure Client から接続すると、Threat Defense によりそれらのカスタマイズがエンドポイントに配布されます。

Secure Client のカスタマイズオブジェクトは、Secure Client をカスタマイズするために使用されるファイルを表します。サポートされている Secure Client のカスタマイズは次のとおりです。

- GUI テキストとメッセージ
- アイコンとイメージ
- スクリプト
- バイナリ
- カスタム インストーラ トランスフォーム
- Localized Installer Transforms

これらの Secure Client のカスタマイズの設定について詳しくは、Cisco Secure Client のカスタマイズ を参照してください。

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、Secure Client プロファイル ファイルや Secure Client イメージ ファイルが含まれます。

また、プロファイルが各 AnyConnect および Secure Client管理 VPN に対して、独立したプロファイルエディタを使用して作成され、Secure Client の一部としてエンドポイント上の管理者定義のエンドユーザー要件および認証ポリシーに展開されます。これにより、エンドユーザーは事前設定済みのネットワークプロファイルを使用できるようになります。

ファイル オブジェクトを作成すると、Firewall 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 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、デバイスの適切なディレクトリにダウンロードされます。

各ファイルに対して次のいずれかのオプションをクリックできます。

- [ダウンロード（Download）]：クリックして Secure Client ファイルをダウンロードします。
- [Edit]：ファイルオブジェクトの詳細を変更します。
- [削除（Delete）]：Secure Client ファイル オブジェクトを削除します。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。

ナビゲーション パス

Objects > **Object Management** > **VPN** > **Secure Client File**。

フィールド

- [Name]：ファイルオブジェクトを識別するファイルの名前を入力します。最大 128 文字まで追加できます。
- [File Name]：[Browse] をクリックしてファイルを選択します。ファイルを選択すると、ファイル名とファイルのフルパスが追加されます。
- [File Type]：選択したファイルに対応するファイルタイプを選択します。次のファイルタイプを使用できます。
  - **[Secure Clientイメージ（Secure Client Image）]**：シスコのソフトウェア ダウンロードセンターからダウンロードした Secure Clientイメージを追加する場合は、このタイプを選択します。

    新規または追加の Secure Clientイメージを、リモートアクセス VPN ポリシーに関連付けることができます。また、サポート対象外または期限切れで不要になったクライアント パッケージの関連付けを解除できます。
  - **[Secure Client VPNプロファイル（Secure Client VPN Profile）]**：Secure Client VPN プロファイルファイルにはこのタイプを選択します。

    プロファイルファイルは、独立した設定ツールである GUIベースの Secure Client プロファイルエディタ を使用して作成されます。詳細については、『Cisco Secure Client

(including AnyConnect) User Guide』の該当するリリースの「*Secure Client* プロファイルエディタ」の章を参照してください。

- [Secure Client管理VPNプロファイル（Secure Client Management VPN Profile）]：Secure Client管理VPNトンネルのプロファイルファイルを追加する場合は、このタイプを選択します。

  シスコのソフトウェア ダウンロードセンターからSecure Client VPN Management Tunnel Standalone Profile Editorをまだダウンロードしていない場合はダウンロードして、管理 Secure Client トンネルに必要な設定を使用してプロファイルを作成します。

- [AMPイネーブラサービスプロファイル（AMP Enabler Service Profile）]：このプロファイルはSecure Client AMP イネーブラに使用されます。リモートアクセス VPN ユーザーが VPN に接続すると、AMP Enabler がこのプロファイルと共に Firewall Threat Defense からエンドポイントにプッシュされます。

- [Feedback Profile]：カスタマーエクスペリエンス フィードバック プロファイルを追加し、このタイプを選択すると、顧客が有効にして使用している機能およびモジュールに関する情報を受信できます。

- [ISEポスチャプロファイル（ISE Posture Profile）]：Secure Client ISE ポスチャモジュールのプロファイルファイルを追加する場合は、このオプションを選択します。

- [NAM Service Profile]：ネットワーク アクセス マネージャのプロファイルエディタを使用して、NAM プロファイルファイルを設定および追加します。

- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：Secure Client Network Visibility Module のプロファイルファイル。NVM プロファイルエディタを使用してプロファイルを作成できます。

- [Umbrella Roaming Security Profile]：プロファイルエディタを使用して作成された .json ファイルを使用してUmbrellaローミングセキュリティモジュールを展開する場合は、このファイルタイプを選択する必要があります。

- [Web Security Service Profile]：Web セキュリティモジュールのプロファイルファイルを追加するときに、このファイルタイプを選択します。

- [Secure Firewall Postureパッケージ（Package）]：Secure Firewall Posture パッケージファイルを追加するときに、このファイルタイプを選択します。このファイルは、エンドポイントにインストールされているオペレーティングシステム、ウイルス対策、スパイウェア対策、およびファイアウォール ソフトウェアに関する情報を収集するために、ダイナミック アクセス ポリシー（DAP）を構成するときに使用されます。

- **[Secure Client外部ブラウザパッケージ（Secure Client External Browser Package）]**：このファイルタイプは、SAML シングルサインオン Web 認証用の外部ブラウザパッケージファイルを選択するためのものです。

  外部パッケージファイルの新しいバージョンが利用可能になったときに、パッケージファイルを追加できます。

  詳細については、「リモートアクセス VPN の AAA 設定」を参照してください。

• [Description]：説明を追加します（オプション）。

関連トピック

Cisco Secure Client イメージ
グループポリシーの Secure Clientオプション （146 ページ）

オブジェクト管理の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
マージされた ACL と AV ACL	7.4.1	任意	新規/変更された画面：**[オブジェクト（Objects）]** > > **[オブジェクト管理（Object Management）]** > **[RADIUSサーバーグループ（RADIUS Server Group）]** > **[RADIUSサーバーグループの追加（Add RADIUS Server Group）]** > **[ダウンロード可能ACLとシスコAVペアACLの結合（Merge Downloadable ACL with Cisco AV Pair ACL）]** 新しい CLI コマンド： • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair**
Secure Client のカスタマイズ	任意（Any）	7.4	Secure Client をカスタマイズして、それらのカスタマイズを VPN ヘッドエンドに展開できるようになりました。エンドユーザーが Secure Client から接続すると、Threat Defense によりそれらのカスタマイズがエンドポイントに配布されます。
CRL および OCSP URL の IPv6 サポート	任意（Any）	7.4	IPv6 OCSP および CRL URL を設定できるようになりました。
ループバックおよび管理タイプのインターフェイス グループ オブジェクト	任意（Any）	7.4	管理専用インターフェイスまたはループバック インターフェイスのみを含むインターフェイス グループ オブジェクトを作成できるようになりました。その後、作成したグループを DNS サーバー、HTTP アクセス、SSH などの管理機能に使用できます。ループバック グループは、ループバック インターフェイスをサポートするすべての機能でサポートされています。DNS では管理インターフェイスはサポートされていません。 新規/変更された画面：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[インターフェイス（Interface）]** > **[追加（Add）]** > **[インターフェイスグループ（Interface Group）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
AAA のループバック インターフェイス サポート	任意（Any）	7.4	Radius サーバーの設定にループバック インターフェイス グループを使用できます。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAAサーバー（AAA Server）] > [Radius サーバーグループ（RADIUS Server Group）]**
ネットワークおよびポートオブジェクトの複製	任意（Any）	7.4	ネットワークおよびポートオブジェクトを複製できるようになりました。オブジェクトマネージャ（**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**）で、ポートまたはネットワークオブジェクトの横にある新しい [クローン（Clone）] アイコンをクリックします。その後、新しいオブジェクトのプロパティを変更し、新しい名前で保存できます。
DHCP IPv6 プール	任意（Any）	7.3	Firewall Threat Defense は、DHCPv6 プレフィックス委任クライアントを使用するときに、軽量の DHCPv6 ステートレスサーバーをサポートするようになりました。SLAAC クライアントが Firewall Threat Defense に情報要求（IR）パケットを送信すると、Firewall Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Firewall Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの追加/編集（Add/Edit Interfaces）] > [IPv6] > [DHCP]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [DHCP IPv6プール（DHCP IPv6 Pool）]** 新規/変更されたコマンド：**show ipv6 dhcp**
BFD テンプレート（BFD Template）	任意（Any）	7.3	以前のリリースでは、BFD は FlexConfig を介してのみ Threat Defense で設定可能でした。FlexConfig は、BFD 設定をサポートしなくなりました。Management Center の UI で Threat Defense の BFD ポリシーを設定できるようになりました。そのため、BFD テンプレートオブジェクトが導入されました。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BFD]**。 • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [BFDテンプレート（BFD Template）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
ポリシーベースルーティング用の新しい[アプリケーション（Applications）] タブ	いずれか	7.1	直接インターネット アクセス ポリシー（ポリシーベースルーティング）を設定するためのアプリケーションを選択できる新しいタブが、拡張アクセスリストオブジェクトに導入されました。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）]**ページ。 サポートされているプラットフォーム： Secure Firewall Management Center
新しい拡張コミュニティ リスト オブジェクトおよび	いずれか	7.1	ポリシーリストおよびルートマップオブジェクトで使用するために、拡張コミュニティ リスト オブジェクトが導入されました。拡張コミュニティ リスト オブジェクトは、仮想ルータの BGP ルートリークサポートにおいて、ルートのインポートまたはエクスポートにのみ適用できます。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [コミュニティリスト（Community List）] > [拡張コミュニティ（Extended Community）]**ページ。 サポートされているプラットフォーム： Secure Firewall Management Center
ポリシーリストオブジェクトおよびルートマップオブジェクトの機能拡張	いずれか	7.1	ポリシーリストおよびルートマップで新しく導入された拡張コミュニティ リスト オブジェクトを選択するためのオプション。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ポリシーリスト（Policy List）] > [コミュニティルール（Community Rule）]**タブおよび**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ルートマップ（Route Map）] > [BGP] > [コミュニティ リスト（Community List）]**タブ。 サポートされているプラットフォーム： Secure Firewall Management Center
Snort 3 の時間ベース ACL のサポート	任意（Any）	7.0	アクセス コントロール ポリシーとプレフィルタポリシーの時間ベースのルールは、Snort 3 でもサポートされています。 サポートされているプラットフォーム： Firewall Threat Defense

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
証明書の登録用のEST	任意（Any）	7.0	証明書の登録用の Enrollment over Secure Transport のサポートが提供されました。 新規/変更された画面：**[オブジェクト（Objects）]** > **[PKI]** > **[証明書の登録（Cert Enrollment）]** > **[CA情報（CA Information）]**タブ。 サポートされているプラットフォーム： Secure Firewall Management Center
EdDSA証明書タイプのサポート	任意（Any）	7.0	新しい証明書キータイプ：EdDSA（キーサイズ 256）が追加されました。 新規/変更された画面：**[オブジェクト（Objects）]** > **[PKI]** > **[証明書の登録（Cert Enrollment）]** > **[キー（Key）]**。 サポートされているプラットフォーム： Secure Firewall Management Center
暗号とキーサイズの制限	任意（Any）	7.0	RSA 暗号化署名アルゴリズムを使用した SHA-1、および RSA キーサイズが 2048 ビット未満の SHA-1 を持つ証明書はサポートされていません。既存の証明書に対するこれらの制限をオーバーライドするには、Firewall Threat Defense で弱い暗号のオプションを有効にします。ただし、サイズが 2048 ビット未満の RSA キーは生成できません。 新規/変更された画面：**[デバイス（Devices）]**>**[証明書（Certificates）]**を設定するときの新しいトグルボタン。 サポートされているプラットフォーム： Secure Firewall Management Center
セキュリティインテリジェンスフィードのオプション	いずれか	6.7	カスタム セキュリティ インテリジェンス フィードの新しい更新頻度オプション（5 分と 15 分）。 更新頻度が 30 分未満の場合は、フィードが変更されていない場合に不要なダウンロードが行われないように、MD5 URL が必要です。 新規/変更された画面：**[セキュリティ インテリジェンス（Security Intelligence）]** > **[ネットワーク リストおよびフィード（Network Lists and Feeds）]**を設定するときの新しい頻度の選択肢。 サポートされているプラットフォーム： Secure Firewall Management Center

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
カンマ区切り値（csv）ファイルを使用したオブジェクトの一括アップロード	いずれか	6.7	オブジェクトは、カンマ区切り値ファイルからインポートできます。1 回の試行で最大 1000 個のオブジェクトをインポートできます。 新規/変更された画面：次のオブジェクトタイプについて、[[オブジェクトタイプ]の追加（Add [Object Type]）] ドロップダウンリストに、新しい [オブジェクトのインポート（Import Object）] オプションがあります。 • **[識別名（Distinguished Name）]** > **[個々のオブジェクト（Individual Objects）]** • **[ネットワーク オブジェクト（Network Object）]** • **ポート（Port）** • **URL** • **VLAN タグ** サポートされているプラットフォーム： Secure Firewall Management Center
インターフェイスオブジェクトが使用されているポリシーの表示	任意（Any）	6.6	インターフェイス オブジェクトが使用されているポリシーを表示します。 新規/変更された画面：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** の **[インターフェイス（Interface）]** オブジェクト ページには新しい **[検索（Find）]** ボタンがあります。 サポートされているプラットフォーム： Secure Firewall Management Center
タイムゾーンオブジェクトの導入	任意（Any）	6.6	時間ベースのポリシーを適用するときに使用するために、タイムゾーンを Firewall Threat Defense デバイスに割り当てることができます。 新規/変更された画面：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**の新しい**[タイムゾーンオブジェクト（Time Zone Object）]**。 サポートされているプラットフォーム： Secure Firewall Management Center

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
アクセスコントロールポリシーとプレフィルタポリシーで時間ベースのオブジェクトが使用可能に	任意（Any）	6.6	アクセス コントロール ポリシーとプレフィルタポリシーで時間ベースのルールを適用するために、時間範囲オブジェクトを新しいタイムゾーンオブジェクトと組み合わせて使用します。 適用するルールの絶対時間または反復時間、あるいは時間範囲を指定できます。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。
プレフィルタルールページからのオブジェクトの詳細の表示	任意（Any）	6.6	導入された機能：プレフィルタルールを表示するときに、オブジェクトまたはオブジェクトグループの詳細を表示するオプション。 新しいオプション：プレフィルタルールリストの次のいずれかの列の値を右クリックすると、オブジェクトの詳細を表示するオプションが提供されます：[送信元ネットワーク（Source Networks）]、[接続先ネットワーク（Destination Networks）]、[送信元ポート（Source Port）]、[接続先ポート（Destination Port）]、および[VLANタグ（VLAN Tag）]。 サポートされているプラットフォーム： Secure Firewall Management Center

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。