基本設定を構成

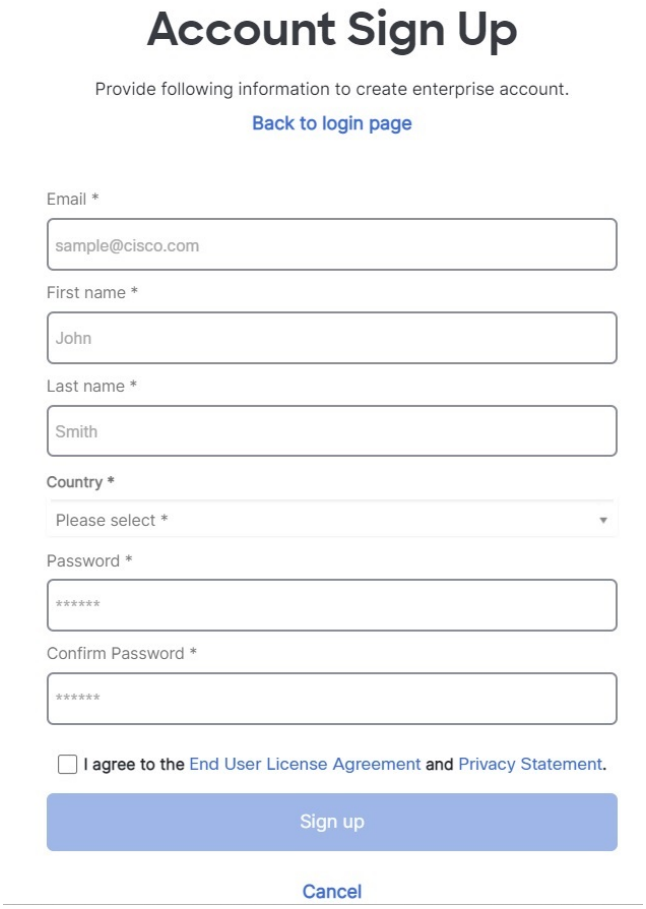
Security Cloud Control は、明確で簡潔なインターフェイスを通じてポリシーを管理するための独自のビューを提供します。Security Cloud Control を初めて使用する場合の基本的な事柄について以下で取り上げます。

Security Cloud Control テナントの作成

新しい Security Cloud Control テナントをプロビジョニングして、デバイスをオンボーディングおよび管理できます。オンプレミス Firewall Management Center バージョン 7.2 以降を使用していて、Cisco Security Cloud と統合する場合は、統合ワークフローの一部として Security Cloud Control テナントを作成することもできます。

手順

1. https://us.manage.security.cisco.com/provisionに進みます。
2. Security Cloud Controlテナントをプロビジョニングするリージョンを選択して、[サインアップ（Sign Up）] をクリックします。
3. [Security Cloud Sign On] ページで、ログイン情報を入力します。
4. Security Cloud Sign On アカウントをお持ちでなく、作成する場合は、[今すぐサインアップ（Sign up now）] をクリックします。
   1. アカウントを作成するための情報を入力します。



次にいくつかのヒントを示します。

- [電子メール（Email）]：Security Cloud Control へのログインに最終的に使用する電子メールアドレスを入力します。
- [パスワード（Password）]：強力なパスワードを入力します。

   2. [サインイン（Sign up）] をクリックします。その後、登録したアドレスに確認メールが送信されます。

3. E メールを開き、E メールと [Security Cloudサインオン（Security Cloud Sign On）] ページの両方で [アカウントのアクティブ化（Activate account）] をクリックします。
4. 任意のデバイスで Duo を使用して多要素認証を設定し、[Duo でログイン（Log in with Duo）] と [終了（Finish）] をクリックします。

（注） Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。

5. テナントの名前を入力し、[新しいアカウントの作成（Create new account）] をクリックします。
6. 選択したリージョンに新しい Security Cloud Control テナントが作成されます。また、作成中の Security Cloud Control テナントに関する詳細が記載された電子メールが届きます。すでに複数の Security Cloud Control テナントに関連付けられている場合は、[テナントの選択（Choose a tenant）]ページで、作成したテナントを選択してログインします。新しい Security Cloud Control テナントを初めて作成した場合は、そのテナントに直接ログインします。

   初めて Security Cloud Control テナントにログオンする方法については、「新規 Security Cloud Control テナントへの初回ログイン」を参照してください。

   Security Cloud Control テナントの管理とさまざまなテナント設定については、「テナント管理」を参照してください。

Security Cloud Control テナントの完全バージョンへのアップグレード

無料トライアルバージョンの Security Cloud Control を使用している場合は、[CDOの無料トライアル期間（You are in a free Trial of Security Cloud Control）] バナーが表示され、トライアル期間の残り日数が示されます。トライアル期間中はいつでも、Security Cloud Control テナントを完全バージョンにアップグレードできます。シスコのセールス担当者またはシスコセールス窓口に連絡してください。代理で発注し、SO 番号を取得します。

SO 番号を取得したら、バナーの [完全バージョンにアップグレード（Upgrade to full version）] をクリックし、注文番号を入力して完全バージョンの Security Cloud Control の使用を開始します。

Security Cloud Control のトライアル期間延長の要求

トライアルバージョンの使用を 30 日間継続する場合は、[延長の要求（Request for an extension）] をクリックします。

Security Cloud Control Firewall Management ダッシュボード

Security Cloud Control Firewall Management ダッシュボードは、さまざまなカテゴリにわたって組織レベルの詳細をモニタリングおよび管理するための中央ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

ダッシュボードをカスタマイズする

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードウィジェットを選択または選択解除し、ドラッグアンドドロップして希望の順序に配置します。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。有効にすると、次のウィジェットが表示できます。

- **設定状態**：デバイス上の設定と、Security Cloud Control によって維持されているデバイス上の設定との不一致を示します。この比較は、存在する可能性のある不整合や競合を特定するのに役立ちます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理**： 変更ログを管理して、正確な運用管理を実現できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「ログの変更」を参照してください。

- **RA VPN セッション**：リモートアクセス VPN セッションをモニターするのに役立ちます。

  詳細については、「RA VPN セッション」を参照してください。

- **全体のインベントリ**：すべてのデバイスの正常性とステータスをモニターするのに役立ちます。ウィジェットには、**[Issues]**、**[Pending Actions]**、**[Other]**、**[Online]** に分類されたデバイス、およびハードウェアサポートの最終日に近づいているデバイス、またはすでにハードウェアサポートの最終日に達しているデバイスが表示されます。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN**： サイト間 VPN 接続を管理および評価するのに役立ちます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

  詳細については、「サイト間 VPN」を参照してください。

- **アカウントとアセット**：
  - マルチクラウドアカウントとリソースを効果的に追跡および管理できます。ここから Multicloud Defense Controller を起動できます。

- **[+Add Account]** をクリックして、新しいアカウントを追加します。

詳細については、「Multicloud Defense コントローラ」を参照してください。

- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。**許可された**トラフィック（デフォルト）と**ブロックされた**トラフィックの間でフィルタ処理できます。
- **上位の侵入およびマルウェアイベント**：上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。**許可されたイベント**（デフォルト）と**ブロックされた**イベントの間でフィルタ処理できます。

アナウンスメント

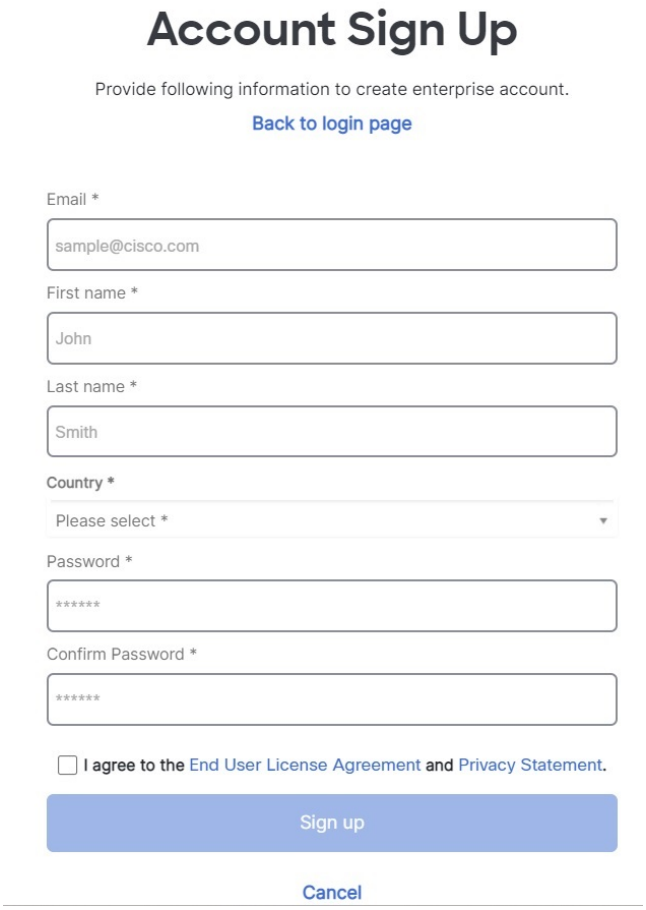
[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目のいずれかについて詳細が必要な場合は、関連ドキュメントへのリンクが提供されます。

Security Cloud Control テナントの作成

新しい Security Cloud Control テナントをプロビジョニングして、デバイスをオンボーディングおよび管理できます。オンプレミス Firewall Management Center バージョン 7.2 以降を使用していて、Cisco Security Cloud と統合する場合は、統合ワークフローの一部として Security Cloud Control テナントを作成することもできます。

手順

1. https://us.manage.security.cisco.com/provisionに進みます。
2. Security Cloud Control テナントをプロビジョニングするリージョンを選択して、[サインアップ（Sign Up）] をクリックします。
3. [Security Cloud Sign On] ページで、ログイン情報を入力します。
4. Security Cloud Sign On アカウントをお持ちでなく、作成する場合は、[今すぐサインアップ（Sign up now）] をクリックします。
   1. アカウントを作成するための情報を入力します。



次にいくつかのヒントを示します。

- [電子メール（Email）]：Security Cloud Control へのログインに最終的に使用する電子メールアドレスを入力します。
- [パスワード（Password）]：強力なパスワードを入力します。

2. [サインイン（Sign up）] をクリックします。その後、登録したアドレスに確認メールが送信されます。
3. E メールを開き、E メールと [Security Cloudサインオン（Security Cloud Sign On）] ページの両方で [アカウントのアクティブ化（Activate account）] をクリックします。
4. 任意のデバイスで Duo を使用して多要素認証を設定し、[Duo でログイン（Log in with Duo）] と [終了（Finish）] をクリックします。

（注） Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。

5. テナントの名前を入力し、[新しいアカウントの作成（Create new account）] をクリックします。
6. 選択したリージョンに新しい Security Cloud Control テナントが作成されます。また、作成中の Security Cloud Control テナントに関する詳細が記載された電子メールが届きます。すでに複数の Security Cloud Control テナントに関連付けられている場合は、[テナントの選択（Choose a tenant）]ページで、作成したテナントを選択してログインします。新しい Security Cloud Control テナントを初めて作成した場合は、そのテナントに直接ログインします。

   初めて Security Cloud Control テナントにログオンする方法については、「新規 Security Cloud Control テナントへの初回ログイン」を参照してください。

   Security Cloud Control テナントの管理とさまざまなテナント設定については、「テナント管理」を参照してください。

Security Cloud Control テナントの完全バージョンへのアップグレード

無料トライアルバージョンの Security Cloud Control を使用している場合は、[CDOの無料トライアル期間（You are in a free Trial of Security Cloud Control）] バナーが表示され、トライアル期間の残り日数が示されます。トライアル期間中はいつでも、Security Cloud Control テナントを完全バージョンにアップグレードできます。シスコのセールス担当者またはシスコセールス窓口に連絡してください。代理で発注し、SO 番号を取得します。

SO 番号を取得したら、バナーの [完全バージョンにアップグレード（Upgrade to full version）] をクリックし、注文番号を入力して完全バージョンの Security Cloud Control の使用を開始します。

Security Cloud Control のトライアル期間延長の要求

トライアルバージョンの使用を 30 日間継続する場合は、[延長の要求（Request for an extension）] をクリックします。

Security Cloud Control Firewall Management ダッシュボード

Security Cloud Control Firewall Management ダッシュボードは、さまざまなカテゴリにわたって組織レベルの詳細をモニタリングおよび管理するための中央ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

ダッシュボードをカスタマイズする

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードウィジェットを選択または選択解除し、ドラッグアンドドロップして希望の順序に配置します。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。有効にすると、次のウィジェットが表示できます。

- **設定状態**：デバイス上の設定と、Security Cloud Control によって維持されているデバイス上の設定との不一致を示します。この比較は、存在する可能性のある不整合や競合を特定するのに役立ちます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理**： 変更ログを管理して、正確な運用管理を実現できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「ログの変更」を参照してください。

- **RA VPN セッション**：リモートアクセス VPN セッションをモニターするのに役立ちます。

  詳細については、「RA VPN セッション」を参照してください。

- **全体のインベントリ**：すべてのデバイスの正常性とステータスをモニターするのに役立ちます。ウィジェットには、**[Issues]**、**[Pending Actions]**、**[Other]**、**[Online]** に分類されたデバイス、およびハードウェアサポートの最終日に近づいているデバイス、またはすでにハードウェアサポートの最終日に達しているデバイスが表示されます。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN**： サイト間 VPN 接続を管理および評価するのに役立ちます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

  詳細については、「サイト間 VPN」を参照してください。

- **アカウントとアセット**：

  - マルチクラウドアカウントとリソースを効果的に追跡および管理できます。ここから Multicloud Defense Controller を起動できます。
  - **[+Add Account]** をクリックして、新しいアカウントを追加します。

  詳細については、「Multicloud Defense コントローラ」を参照してください。

- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。**許可されたトラフィック**（デフォルト）と**ブロックされた**トラフィックの間でフィルタ処理できます。

- **上位の侵入およびマルウェアイベント**： 上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。**許可されたイベント**（デフォルト）と**ブロックされた**イベントの間でフィルタ処理できます。

アナウンスメント

[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目のいずれかについて詳細が必要な場合は、関連ドキュメントへのリンクが提供されます。

Security Cloud Control のログイン要件

Security Cloud Control にログインするには、SAML 2.0 準拠のアイデンティティ プロバイダー（IdP）、多要素認証プロバイダー、および Security Cloud Control のユーザーレコードを持つアカウントが必要です。

IdP アカウントにはユーザーのログイン情報が含まれており、IdP はそのログイン情報に基づいてユーザーを認証します。多要素認証では、アイデンティティセキュリティの付加的なレイヤが提供されます。Security Cloud Control ユーザーレコードには、主にユーザー名、ユーザーが関連付けられる Security Cloud Control テナント、ユーザーのロールが含まれます。ユーザーがログインすると、Security Cloud Control は IdP のユーザー ID を Security Cloud Control のテナントの既存ユーザーレコードにマッピングします。Security Cloud Control が一致するレコードを見つけた場合に、該当するユーザーはそのテナントへのログインを許可されます。

お客様の企業に独自のシングルサインオン アイデンティティ プロバイダーがない限り、アイデンティティ プロバイダーは Security Cloud Sign On です。Security Cloud Sign On は、多要素認証に Duo を使用します。

お客様は、必要に応じて自分の IdP を Security Cloud Control と統合できます。

Security Cloud Control にログインするには、まず Cisco Security Cloud Sign On でアカウントを作成し、Duo Security を使用して多要素認証（MFA）を設定し、テナントのネットワーク管理者に Security Cloud Control レコードの作成を依頼する必要があります。

2019 年 10 月 14 日、Security Cloud Control は、既存のすべてのテナントを、アイデンティティ プロバイダーとして Cisco Security Cloud Sign On を使用し、MFA に Duo を使用するように変換しました。

（注）

- 独自のシングルサインオン ID プロバイダーを使用して Security Cloud Control にサインインする場合、この Cisco Security Cloud Sign On への移行は影響しません。独自のサインオンソリューションを引き続き使用できます。
- Security Cloud Control の無料試用期間中であれば、この移行の影響はあります。

Security Cloud Control テナントが 2019 年 10 月 14 日以降に作成された場合は、新規 Security Cloud Control テナントへの初回ログイン （10 ページ）を参照してください。

2019 年 10 月 14 日より前に Security Cloud Control テナントが存在していた場合は、Cisco Security Cloud Sign On ID プロバイダーへの移行 （11 ページ）を参照してください。

新規 Security Cloud Control テナントへの初回ログイン

はじめる前に

Duo Security のインストール。Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。

時刻の同期。モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが自動的に、または手動で正しい時刻に設定されていることを確認します。

Security Cloud Control は、Cisco Security Cloud Sign On を ID プロバイダーとして使用し、Duo を多要素認証（MFA）に使用します。Cisco Security Cloud Sign On アカウントがない場合に新しい Security Cloud Control テナントを作成すると、プロビジョニングフローには、Security Cloud Sign On アカウントの作成や Duo を使用した MFA の設定など、さまざまな手順が必要になります。新しいテナントを作成するには、こちらをクリックしてください。

MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、Security Cloud Control にログインするユーザーのアイデンティティを確認するために、2 つのコンポーネントまたは要素が必要です。最初の要素はユーザー名とパスワードで、2番目の要素はオンデマンドで生成されるワンタイムパスワード（OTP）です。

重要 **2019 年 10 月 14 日より前に Security Cloud Control テナントが存在していた場合は**、この項目の代わりにCisco Security Cloud Sign On ID プロバイダーへの移行 （11 ページ）をログイン手順として使用してください。

次の手順

新規 Cisco Security Cloud Sign On アカウントの作成と Duo 多要素認証の設定 に進みます。これは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

リージョンごとの Security Cloud Control へのサインイン

こちらは、Security Cloud Control へのサインインに使用する AWS リージョンごとの URL です。

表 *1*：リージョンごとの *Security Cloud Control URL*

地域	Security Cloud Control URL
アジア太平洋および日本（APJ）	https://apj.manage.security.cisco.com
オーストラリア（AUS）	https://aus.manage.security.cisco.com

地域	Security Cloud Control URL
ヨーロッパ、中東、アフリカ（EMEA）	https://eu.manage.security.cisco.com
インド（IN）	https://in.manage.security.cisco.com
アメリカ合衆国（US）	https://us.manage.security.cisco.com

ログインの失敗のトラブルシューティング

正しくない Security Cloud Control リージョンに誤ってログインしているため、ログインに失敗する

適切な Security Cloud Control リージョンにログインしていることを確認してください。https://sign-on.security.cisco.com にログインすると、アクセスするリージョンを選択できます。

サインインするリージョンについては、リージョンごとの Security Cloud Control へのサインイン （10 ページ） を参照してください。

Cisco Security Cloud Sign On ID プロバイダーへの移行

2019 年 10 月 14 日時点で、Security Cloud Control では、すべてのテナントがアイデンティティプロバイダーとして Cisco Security Cloud Sign On に変換されており、多要素認証（MFA）には Duo を使用しています。**Security Cloud Control にログインするには、まず Cisco Secure Sign-On でアカウントをアクティブ化し、Duo を使用して MFA を設定する必要があります。**

Security Cloud Control には MFA が必要です。MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、Security Cloud Control にログインするユーザーの ID を確認するために、2 つのコンポーネントまたは要素が必要です。最初の要素はユーザー名とパスワードで、2 番目の要素はオンデマンドで生成されるワンタイムパスワード（OTP）です。

（注）

- 独自のシングルサインオン ID プロバイダーを使用して Security Cloud Control にサインインする場合、この Cisco Security Cloud Sign On および Duo への移行は影響しません。独自のサインオンソリューションを引き続き使用できます。
- Security Cloud Control の無料トライアル期間中であれば、この移行が適用されます。
- **2019 年 10 月 14 日以降に Security Cloud Control テナントが作成されていた場合は、**この項目の代わりに新規 Security Cloud Control テナントへの初回ログイン （10 ページ）をログイン手順として使用してください。

はじめる前に

移行する前に、次の手順を実行することを強くお勧めします。

- **Duo Security のインストール。**Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。
- **時刻の同期。**モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが自動的に、または手動で正しい時刻に設定されていることを確認します。
- 「新規 Cisco Security Cloud Sign On アカウントの作成と Duo 多要素認証の設定」。これは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

移行後のログイン失敗のトラブルシューティング

ユーザー名またはパスワードが正しくないため、Security Cloud Control へのログインに失敗する

解決法 Security Cloud Control にログインしようとして、知っている正しいユーザー名とパスワードを使用しているにもかかわらずログインに失敗する場合、または「パスワードを忘れた場合」を試しても有効なパスワードを回復できない場合は、新しい Cisco Security Cloud Sign On アカウントを作成せずにログインを試みた可能性があります。新しい Cisco Security Cloud Sign On アカウントにサインアップする必要があります。

解決法 新規 Cisco Security Cloud Sign On アカウントの作成と Duo 多要素認証の設定を参照してください。

Cisco Security Cloud Sign On ダッシュボードへのログインは成功するが、Security Cloud Control を起動できない

解決法 Security Cloud Control テナントとは異なるユーザー名で Cisco Security Cloud Sign On アカウントを作成している可能性があります。Security Cloud Control と Cisco Secure Sign-On の間でユーザー情報を標準化するには、Cisco Technical Assistance Center（TAC）に連絡してください。

保存したブックマークを使用したログインに失敗する

解決法 ブラウザに保存された古いブックマークを使用してログインしようとしているかもしれません。ブックマークが https://cdo.onelogin.com を指している可能性があります。

解決法 https://sign-on.security.cisco.com にログインします。

- **解決法** Cisco Secure Sign-On アカウントをまだ作成していない場合は、アカウントを作成します。
- **解決法** Cisco Secure Sign-On の新規アカウントを作成した場合は、テナントが作成されたリージョンに対応するダッシュボードの Security Cloud Control タイルをクリックします。

- **解決法** Security Cloud Control APJ
- **解決法** Security Cloud Control オーストラリア
- **解決法** Security Cloud Control EU
- **解決法** Security Cloud Control インド
- **解決法** Security Cloud Control 米国

- **解決法** https://sign-on.security.cisco.com を指すようにブックマークを更新します。

Security Cloud Control テナントの起動

手順

ステップ 1 Cisco Security Cloud Sign On ダッシュボードで、該当するリージョンの Security Cloud Control ボタンをクリックします。

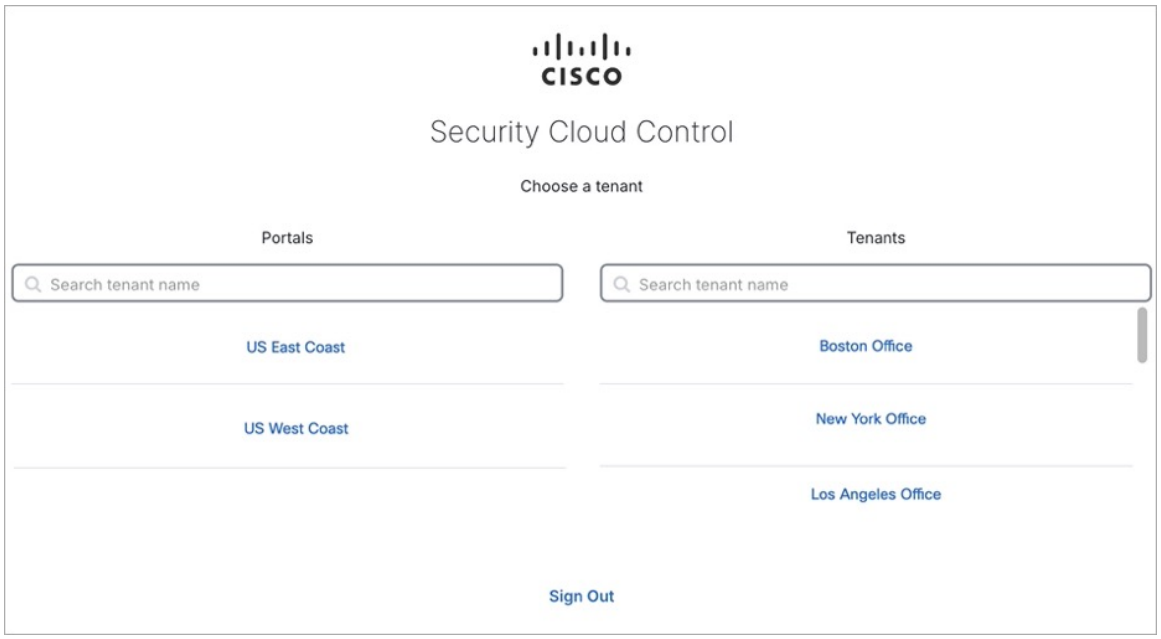
ステップ 2 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

- 既存のテナントにすでにユーザーレコードがある場合は、そのテナントにログインします。
- 複数のポータルにすでにユーザーレコードがある場合は、接続するポータルを選択できます。
- すでに複数のテナントにユーザーレコードがある場合は、接続先の Security Cloud Control テナントを選択できます。
- 既存のテナントにユーザーレコードがない場合は、Security Cloud Control の詳細を確認するか、またはトライアルテナントを要求できます。

[ポータル（Portals）] ビューは、複数のテナントから統合された情報を取得して表示します。

詳細については、MSSP ポータルを参照してください。

[テナント（Tenant）] ビューには、ユーザーレコードがある一部のテナントが表示されます。



Security Cloud Control Firewall Management[Integration] ページ

[Integration] ページでは、Security Cloud Control Firewall Management 内の管理対象インフラストラクチャの包括的なビューが表示されます。

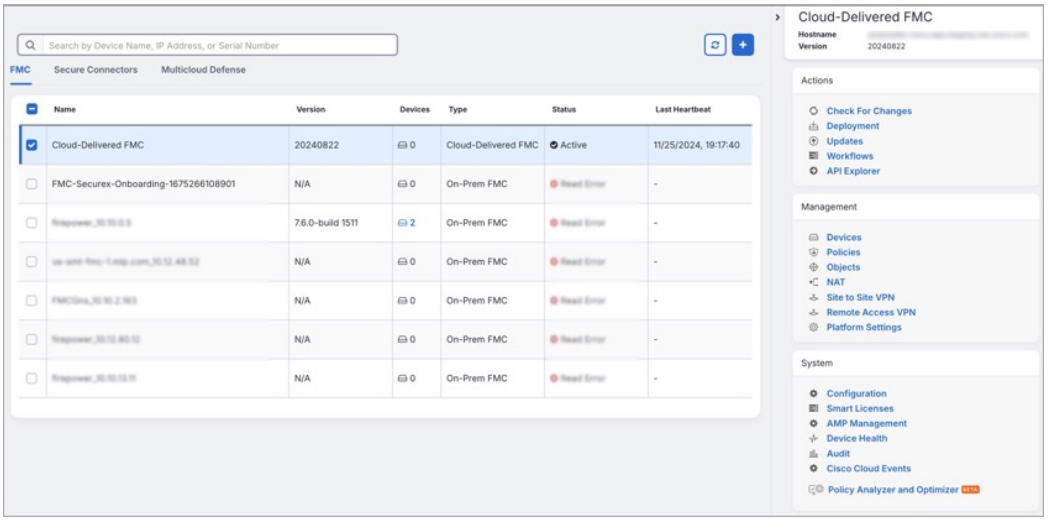
- **[FMC]** タブ：
  - Security Cloud Control Firewall Management アカウントにリンクされている クラウド提供型 Firewall Management Center を提供します。「Security Cloud Control テナントのクラウド提供型 Firewall Management Center のリクエスト」を参照してください。
  - Security Cloud Control Firewall Management にオンボーディングされた オンプレミス Firewall Management Center を一覧表示します。これらの オンプレミス Firewall Management Center によって管理されるデバイスは、**[Security Devices]** にリストされています。「Security Cloud Control を使用したオンプレミス Firewall Management Center の管理」を参照してください。
  - **[Secure Connectors]** の下に **Secure Device Connector** と **Secure Event Connector**を表示します。「Secure Device Connector」および「Secure Event Connector」を参照してください。

Security Cloud Control ページ。**[Integration]** ページにもタブが含まれます。

[FMC] タブをクリックし、[**Onboard** FMC] アイコンをクリックして オンプレミス Firewall Management Center をオンボーディングし、右側のペインのオプションを使用してデバイスアクションを実行できます。「オンプレミス Firewall Management Center のオンボード」を参照してください。

また、バージョン、Management Center で管理されているデバイスの数、デバイスタイプ、デバイスの同期ステータスなどのデバイス情報を確認することもできます。管理対象デバイスのアイコンをクリックすると、**[Security Devices]** ページが表示され、選択した オンプレミス Firewall Management Center によって管理されているデバイスが自動的にフィルタリングされて表示されます。**[Integration]** ページでは、一度に複数の オンプレミス Firewall Management Center を選択して、Management Center のグループですべて一度にアクションを実行することもできます。クラウド提供型 Firewall Management Center が選択されている間は、オンプレミス Firewall Management Center を選択できません。新しいセキュアコネクタを追加したり、既存のセキュアコネクタでアクションを実行したりするには、[セキュアコネクタ（Secure Connectors）] タブを選択して をクリックします。

左側のペインで **[管理（Administration）]** > **[Firewall Management Center]** をクリックします。



クラウド提供型 Firewall Management Center の場合、[Integrations] ページには次の情報が表示されます。

- テナントに クラウド提供型 Firewall Management Center が展開されていない場合は、[クラウド提供型FMCの有効化（Enable Cloud-Delivered FMC）] をクリックします。詳細については、「Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control Tenant」[英語] を参照してください。
- クラウド提供型 Firewall Management Center に展開された Cisco Secure Firewall Threat Defense デバイスの数。
- Security Cloud Control と クラウド提供型 Firewall Management Center ページ間の接続のステータス。

- クラウド提供型 Firewall Management Center の最後のハートビート。これは、クラウド提供型 Firewall Management Center 自体のステータスと管理するデバイスの数がこのページのテーブルと最後に同期された時刻を表します。
- 選択した クラウド提供型 Firewall Management Center のホスト名。

[クラウド提供型FMC（Cloud-Delivered FMC）] を選択し、[アクション（Actions）]、[管理（Management）]、または [設定（Settings）] ペインのリンクを使用して クラウド提供型 Firewall Management Center ユーザーインターフェイスを開き、クリックしたリンクに関連付けられている設定タスクを実行します。

[アクション（Actions）] :

- [変更の確認（Check For Changes）] : テーブルのデバイス数とステータスの情報は、このページと クラウド提供型 Firewall Management Center が最後に同期されたときに使用可能な情報で更新されます。同期は 10 分ごとに行われます。
- [展開（Deployment）] : クラウド提供型 Firewall Management Center のデバイス設定展開ページが表示されます。「設定変更の展開」を参照してください。
- [ワークフロー（Workflows）] : デバイスと通信するときに Security Cloud Control が実行するすべてのプロセスをモニターするための、[ワークフロー（Workflows）] ページが表示されます。「[ワークフロー（Workflows）] ページ」を参照してください。 https://docs.defenseorchestrator.com/#!c-workflows-page.html
- [APIエクスプローラ（API Explorer）] : クラウド提供型 Firewall Management Center の REST API が一覧表示されるページが表示されます。Secure Firewall Management Center REST API のガイドを参照してください。
- **[統合イベント（Unified Events）]** : クラウド提供型 Firewall Management Center ポータルの **[Unified Events]** ページに移動します。このページでは、接続、侵入、ファイル、マルウェア、セキュリティ関連の接続イベントなど、さまざまなファイアウォールイベントが単一の画面に表示されます。詳細については、「統合イベント」を参照してください。

（注） 統合イベント（Unified Events）機能にはアクティベーションが必要です。この機能をまだアクティベートしていない場合は、Cisco の営業担当者に連絡して有効にしてください。

[管理（Management）] :

- [デバイス（Devices）] : クラウド提供型 Firewall Management Center ポータルの Firewall Threat Defense デバイス一覧表示ページが表示されます。「Configure Devices」を参照してください。
- [ポリシー（Policies）] : システム付属のアクセス コントロール ポリシーを編集したり、カスタム アクセス コントロール ポリシーを作成したりするための、クラウド提供型 Firewall Management Center ポータルのポリシーページが表示されます。「Manage Access Control Policies」を参照してください。

- [オブジェクト（Objects）]：再利用可能オブジェクトを管理するための、クラウド提供型 Firewall Management Center ポータルのポリシーページが表示されます。「Object Management」を参照してください。
- [NAT]：Firewall Threat Defense デバイスでネットワークアドレス変換ポリシーを設定するための、クラウド提供型 Firewall Management Center ポータルのポリシーページが表示されます。「Manage NAT policies」を参照してください。
- [サイト間VPN（Site to Site VPN）]：2 つのサイト間のサイト間 VPN ポリシーを設定するための、クラウド提供型 Firewall Management Center ポータルのサイト間 VPN ダッシュボードページが表示されます。「Site-to-Site VPNs」を参照してください。
- [リモートアクセスVPN（Remote Access VPN）]：リモートアクセス VPN 設定を指定するための、クラウド提供型 Firewall Management Center ポータルのリモートアクセス VPN ダッシュボードページが表示されます。「Remote Access VPN」を参照してください。
- **[プラットフォーム設定（Platform Settings）]**：互いに関連しないさまざまな機能を設定し、いくつかのデバイス間でその値を共有するための、クラウド提供型 Firewall Management Center ポータルのプラットフォーム設定ページが表示されます。「Platform Settings」を参照してください。

[システム（System）]：

- [設定（Configuration）]：システム構成設定を指定するための、クラウド提供型 Firewall Management Center ポータルのシステム設定ページが表示されます。「System Configuration」を参照してください。
- [スマートライセンス（Smart Licenses）]：デバイスにライセンスを割り当てるための、クラウド提供型 Firewall Management Center ポータルのスマートライセンスページが表示されます。「Assign Licenses to Devices」を参照してください。
- [AMP管理（AMP Management）]：ネットワーク上のマルウェアを検出してブロックするためにシステムが使用するインテリジェンスを提供する、クラウド提供型 Firewall Management Center ポータルの AMP 管理ページが表示されます。「Cloud Connections for Malware Protection」を参照してください。
- [デバイスの正常性（Device Health）]：さまざまな正常性インジケータを追跡してシステムのハードウェアおよびソフトウェアの正常な動作を確保する、クラウド提供型 Firewall Management Center ポータルのヘルスモニタリングページが表示されます。「About Health Monitoring」を参照してください。
- [監査（Audit）]：Web インターフェイスとユーザーとの対話のそれぞれに対して生成される監査レコードを表示するための、クラウド提供型 Firewall Management Center ポータルの監査ログページが表示されます。
- [Cisco Cloudイベント（Cisco Cloud Events）]：イベントを SAL（SaaS）に直接送信するように クラウド提供型 Firewall Management Center を設定するための、Security Cloud Control ポータルの Cisco Cloud イベント設定ページが表示されます。「Send Events to SAL (SaaS)」を参照してください。

-

クラウド提供型 Firewall Management Center で、青い疑問符ボタンをクリックし、[ページレベルのヘルプ（Page-level Help）] を選択して、表示しているページの詳細と、さらに実行できるアクションを確認します。

異なるタブで Security Cloud Control と クラウド提供型 Firewall Management Center アプリケーションを開く機能のサポート

Firewall Threat Defense デバイスまたはオブジェクトを クラウド提供型 Firewall Management Center で設定するときに、追加のブラウザタブで適切な設定ページを開いて、ログオフせずに Security Cloud Control と クラウド提供型 Firewall Management Center ポータルで同時に作業できます。

たとえば、クラウド提供型 Firewall Management Center でオブジェクトを作成し、同時にセキュリティポリシーから生成されたイベントログを Security Cloud Control でモニターできます。

この機能は、クラウド提供型 Firewall Management Center ポータルに移動するすべての Security Cloud Control リンクで使用できます。新しいタブで クラウド提供型 Firewall Management Center ポータルを開くには、次の手順を実行します。

Security Cloud Control ポータルで、Ctrl（Windows）または Command（Mac）ボタンを押したまま、対応するリンクをクリックします。

（注） 1 回クリックすると、同じタブで クラウド提供型 Firewall Management Center ページが開きます。

新しいタブで クラウド提供型 Firewall Management Center ポータルページを開く例を次に示します。

- **[Administration]** > **[Firewall Management Center]** を選択し、**[Cloud-Delivered FMC]** を選択します。右側のペインで、Ctrl（Windows）または Command（Mac）ボタンを押したまま、アクセスするページをクリックします。
- [オブジェクト（Objects）] > [その他のFTDオブジェクト（Other FTD Objects）] を選択します。
- Security Cloud Control ページの右上隅にある検索アイコンをクリックし、表示される検索フィールドに検索文字列を入力します。

  検索結果から、Ctrl（Windows）または Command（Mac）ボタンを押したまま、矢印アイコンをクリックします。
- **[Dashboard]**、**[Quick Actions]** の順に選択します。Ctrl（Windows）または Command（Mac）ボタンを押したまま、**[Manage FTD Policies]** または **[Manage FTD Objects]** をクリックします。

（注） 新しい Security Cloud Control テナントに切り替えると、新しいタブですでに開いている対応する クラウド提供型 Firewall Management Center ポータルがログアウトします。

Security Cloud Control Firewall Management ライセンス

Security Cloud Control Firewall Management では、組織の資格の基本サブスクリプションと、デバイスを管理するためのデバイスライセンスが必要です。必要なテナント数に基づいて1つ以上の Security Cloud Control Firewall Management 基本サブスクリプションを購入し、デバイスモデル番号と数量に基づいてデバイスライセンスを購入できます。つまり、基本サブスクリプションを購入すると Security Cloud Control Firewall Management 組織が提供されます。Security Cloud Control Firewall Management を使用して管理することを選択したデバイスごとに、個別のデバイスライセンスが必要です。

Security Cloud Control Firewall Management からデバイスをオンボードして管理するには、管理するデバイスに基づいて、基本サブスクリプションとデバイス固有の期間ベースのサブスクリプションを購入する必要があります。

サブスクリプション

Security Cloud Control Firewall Management サブスクリプションは期間ベースです。

- **基本**：1 年、3 年、および 5 年のサブスクリプションを提供して、Security Cloud Control Firewall Management テナントにアクセスし、適切にライセンスされたデバイスを搭載する資格を提供します。
- **デバイスライセンス**：管理することを選択したサポート対象デバイスについて、1 年、3 年、および 5 年のサブスクリプションを提供します。たとえば、Cisco Firepower 1010 デバイスの 3 年のソフトウェア サブスクリプションを購入した場合、Security Cloud Control Firewall Management を使用して Cisco Firepower 1010 デバイスを 3 年間管理することを選択できます。

Security Cloud Control Firewall Management がサポートするシスコのセキュリティデバイスの詳細については、「Security Cloud Control Firewall Management でサポートされるソフトウェアとハードウェア」を参照してください。

重要 Security Cloud Control Firewall Management の高可用性デバイスペアを管理するために、2 つの個別のデバイスライセンスは必要ありません。 の高可用性ペアがある場合、Security Cloud Control Firewall Management では高可用性デバイスのペアを 1 つのデバイスと見なすため、1 つの デバイスライセンスを購入するだけで十分です。

（注）

- Catalyst SD-WAN には Security Cloud Control Firewall Management と統合するために追加のライセンスは必要ありません。Cisco Digital Network Architecture（DNA）または WAN Essentials ライセンスを持つお客様は、他のライセンスは必要なく、これらの既存のライセンスを統合に使用できます。
-

（注） Cisco Smart Licensing ポータルから Security Cloud Control Firewall Management ライセンスを管理することはできません。

ソフトウェア サブスクリプションのサポート

Security Cloud Control Firewall Management 基本サブスクリプションには、サブスクリプション期間中有効なソフトウェア サブスクリプション サポートが含まれており、ソフトウェアアップデート、メジャーアップグレード、および Cisco Technical Assistance Center（TAC）へのアクセスが追加料金なしで利用できます。ソフトウェアサポートがデフォルトで選択されていますが、要件に基づいて Security Cloud Control Firewall Management ソリューションサポートを活用することもできます。

クラウド提供型 Firewall Management Center ライセンスと登録

クラウド提供型 Firewall Management Center の場合と同じように、オンプレミス Firewall Management Center を Cisco Smart Licensing に登録します。

概要

クラウド提供型 Firewall Management Center は、Security Cloud Control Firewall Management の基本サブスクリプションおよびトライアルに含まれています。クラウド提供型 Firewall Management Center のライセンスを個別に購入する必要はありません。基本サブスクリプションまたはトライアルは クラウド提供型 Firewall Management Center をカバーしており、クラウドを介して Firewall Threat Defense のデバイスを管理できます。

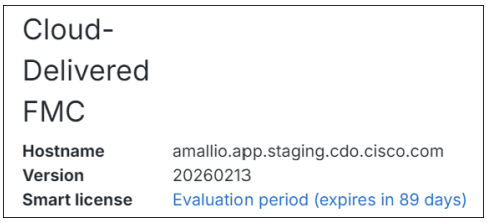
クラウド提供型 Firewall Management Center には 90 日間の評価ライセンスがプロビジョニングされています。

重要 RAVPN や SSL VPN などのエクスポート暗号化を必要とする機能を含むすべての機能にアクセスするには、展開後すぐに Cisco Smart Software Manager に クラウド提供型 Firewall Management Center を登録することを強く推奨します。早期登録により、機能の制限や展開の中断が防止されます。

評価ライセンス

- リモートアクセス VPN、SSL VPN、およびその他の暗号化依存オプションなど、エクスポート暗号化を必要とする機能は、クラウド提供型 Firewall Management Center を Cisco Smart Software Manager（CSSM）に登録するまで無効のままです。
- 90 日間の評価期間が終了した後も、Firewall Threat Defense デバイスのオンボーディングを続行できますが、CSSM への登録が完了するまで、手動でトリガーされた展開またはスケジュールされた展開はブロックされます。
- 評価ライセンスの有効期限が近づいている場合、Security Cloud Control Firewall Management はアラート通知を送信します。

（注） 評価ライセンスの期限が切れると、[スマートライセンス（Smart license）] フィールドに警告が表示されます。



評価期間が終了すると、クラウド提供型 Firewall Management Center は登録解除されます。Cisco Smart Software Manager に クラウド提供型 Firewall Management Center を登録すると、評価モードから完全にライセンスされた状態に変換されます。

評価警告のリンクをクリックしてスマートライセンシングの登録ページを開き、クラウド提供型 Firewall Management Center を Cisco Smart Software Manager に登録します。

Cisco Smart Software Manager（CSSM）

- クラウド提供型 Firewall Management Center と同じプロセスに従って、オンプレミス Firewall Management Center をスマート ライセンス アカウントに接続します。このセクションでは、手順の概要を示します。
- クラウド提供型 Firewall Management Center に対してライセンスを個別に購入する必要はありません。ライセンスは登録時に自動的に適用されます。
- スマートライセンスに登録すると、暗号化エクスポート機能が有効になります。
- 登録すると、コンプライアンスが保証され、展開の問題が防止されます。

Security Cloud Control テナントでプロビジョニングされた クラウド提供型 Firewall Management Center を取得する方法については、「Request a クラウド提供型 Firewall Management Center for your Security Cloud Control Tenant」を参照してください。

Firewall Threat Defense デバイスのライセンス

- クラウド提供型 Firewall Management Center には、ライセンスを個別に購入する必要はありません。
- クラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense デバイスにはそれぞれ個別のライセンスが必要です。
- クラウド提供型 Firewall Management Center を CSSM に登録すると、管理者はセキュリティデバイスに機能ライセンスを適用できます。

登録ステップバイステップ

手順の概要は次のとおりです。詳細は「スマート ソフトウェア マネージャーで管理センターを登録する」を参照してください。

1. スマートアカウントの作成またはアクセス：

   Cisco Smart Software Manager アカウントを持っていることを確認します。次がない場合は、Smart Software Manager で作成します。

2. 登録トークンの生成または登録トークンの使用：

   Smart Software Manager で、既存の有効な登録トークンを使用するか、クラウド提供型 Firewall Management Center を登録する仮想アカウントの登録トークンを生成します。

   1. **[Inventory] > [New Token]** の順に選択します。
   2. 説明を入力し、有効期限を設定します（シスコでは 30 日を推奨）。
   3. トークンを作成し、コピーします。

3. クラウド提供型 Firewall Management Center をトークンに登録します。

   1. クラウド提供型 Firewall Management Center インターフェイスにログインします。
   2. **[System] > [Licenses] > [Smart Licenses]** に移動します。
   3. **[Register]** をクリックし、**[Product Instance Registration Token]** フィールドに登録トークンを貼り付けます。
   4. トークンの前後に余分なスペースや空白行がないことを確認してください。
   5. [変更を適用（Apply Changes）] をクリックします。

4. 登録の確認

   登録後、**[System] > [Licenses] > [Smart Licenses]** でライセンスステータスを確認し、登録が成功し、ライセンスが適用され、「輸出規制機能」が有効になっていることを確認します。

Security Cloud Control Firewall Management プラットフォームのメンテナンススケジュール

Security Cloud Control Firewall Management は、新機能と品質の改善により、プラットフォームを毎週更新します。更新は、このスケジュールに従って 3 時間以内に行われます。

Day of the week	**時刻** **（24 時間表記、UTC）**
Thursday	09:00 UTC - 12:00 UTC

Security Cloud Control Firewall Management のアップグレード期間中も、引き続き組織と クラウド提供型 Firewall Management Center にアクセスできます。さらに、Security Cloud Control Firewall Management にオンボーディングしたデバイスは、引き続きセキュリティポリシーを適用します。

（注）

- Security Cloud Control Firewall Management のメンテナンス期間中は、管理対象デバイスへの設定の作成またはデプロイを行わないでください。
- Security Cloud Control Firewall Management の通信を停止する障害が発生した場合、その障害に対しては、メンテナンス期間外であっても、Cisco は影響を受けるすべてのテナントで可能な限り迅速に対処いたします。

クラウド提供型 Firewall Management Center メンテナンススケジュール

組織に クラウド提供型 Firewall Management Center をデプロイしているお客様には、Security Cloud Control で クラウド提供型 Firewall Management Center 環境が更新される約 1 週間前に通知されます。

テナントのネットワーク管理者および管理者ユーザーには、電子メールで通知が届きます。また、Security Cloud Control のホームページにも、すべてのユーザーに今後の更新を通知するバナーが表示されます。

（注）

- クラウド提供型Firewall Management Centerのメンテナンス期間中は、管理対象デバイスへの設定の作成またはデプロイを行わないでください。
- Security Cloud Control またはクラウド提供型 Firewall Management Center の通信を停止する障害が発生した場合、その障害に対しては、メンテナンス期間外であっても、影響を受けるすべてのテナントで可能な限り迅速に対処いたします。

オブジェクトの概要

オブジェクトは、1つ以上のセキュリティポリシーで使用できる情報のコンテナです。オブジェクトを使用すると、ポリシーの一貫性を簡単に維持できます。単一のオブジェクトを作成し、異なるポリシーを使用して、オブジェクトを変更すると、その変更がオブジェクトを使用するすべてのポリシーに伝播されます。オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

デバイスをオンボードすると、Security Cloud Control はそのデバイスで使用されるすべてのオブジェクトを認識して保存し、[オブジェクト（Objects）] ページにリストします。[オブジェクト（Objects）] ページから、既存のオブジェクトを編集したり、セキュリティポリシーで使用する新しいオブジェクトを作成したりできます。

Security Cloud Control は、複数のデバイスで使用されるオブジェクトを**共有オブジェクト**と呼び、[オブジェクト（Objects）] ページでこのバッジ でそれらを識別します。

共有オブジェクトが何らかの「問題」を引き起こし、複数のポリシーまたはデバイス間で完全に共有されなくなる場合があります。

- **重複オブジェクト**とは、同じデバイス上にある、名前は異なるが値は同じである2つ以上のオブジェクトです。通常、重複したオブジェクトは同じ目的を果たし、さまざまなポリシーによって使用されます。重複するオブジェクトは、この問題のアイコン で識別されます。
- **不整合オブジェクト**とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーは、さまざまな設定の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。不整合オブジェクトは、この問題のアイコン で識別されます。
- **未使用オブジェクト**は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NATルールによって参照されていないオブジェクトです。未使用オブジェクトは、この問題のアイコン で識別されます。

ルールやポリシーですぐに使用するためのオブジェクトを作成することもできます。ルールやポリシーに関連付けないオブジェクトを作成できます。関連付けられていないオブジェクトを

ルールまたはポリシーで使用すると、Security Cloud Control ではそのコピーが作成され、そのコピーが使用されます。

[オブジェクト（Objects）] メニューに移動するか、ネットワークポリシーの詳細でオブジェクトを表示することにより、Security Cloud Control によって管理されているオブジェクトを表示できます。

Security Cloud Control を使用すると、サポートされているデバイス全体のネットワークオブジェクトとサービスオブジェクトを 1 つの場所から管理できます。Security Cloud Control を使用すると、次の方法でオブジェクトを管理できます。

- さまざまな基準に基づいて、すべてのオブジェクトを検索してフィルタリングします。
- デバイス上の重複、未使用、および不整合のオブジェクトを見つけて、それらのオブジェクトの問題を統合、削除、または解決します。
- 関連付けられていないオブジェクトを見つけて、それらが未使用であれば削除します。
- デバイス間で共通の共有オブジェクトを検出します。
- 変更をコミットする前に、オブジェクトへの変更が一連のポリシーとデバイスに与える影響を評価します。
- 一連のオブジェクトとそれらの関係を、さまざまなポリシーやデバイスで比較します。
- デバイスが Security Cloud Control にオンボードされた後、デバイスによって使用されているオブジェクトをキャプチャします。

オンボードされたデバイスからのオブジェクトの作成、編集、または読み取りで問題が発生した場合は、『Security Cloud Control のトラブルシューティング』を参照してください。

オブジェクト タイプ

以下の表では、デバイス用に作成し、Security Cloud Control を使用して管理できるオブジェクトについて説明します。

表 2 : オンプレミスの *Cisco Secure Firewall Management Center* のオブジェクトタイプ

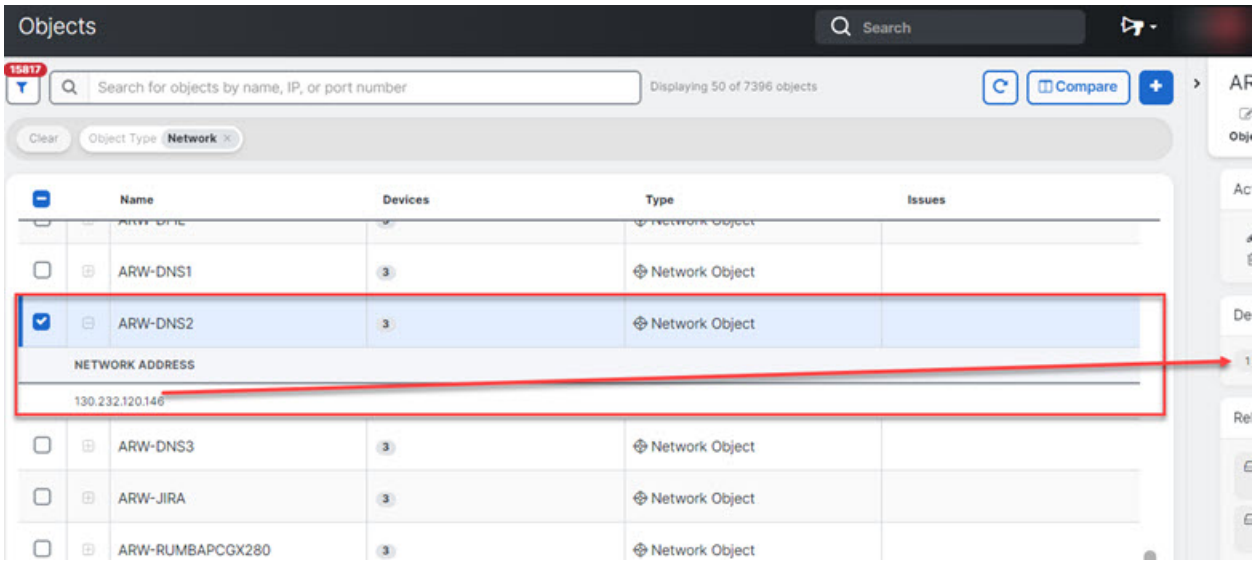
オブジェクト	説明
ネットワーク（Network）	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。
サービス	サービスオブジェクト、サービスグループ、ポートグループは、TCP/IP プロトコルスイートの一部が考慮されたプロトコルまたはポートを含む再利用可能なコンポーネントです。

共有オブジェクト

Security Cloud Control では、複数のデバイス上の同じ名前と同じ内容のオブジェクトを「共有オブジェクト」と呼びます。共有オブジェクトはこのアイコンで識別されます。

これは、[オブジェクト（Objects）]ページに表示されます。共有オブジェクトを使用すると、1 ヵ所でオブジェクトを変更でき、その変更がそのオブジェクトを使用する他のすべてのポリシーに影響するため、ポリシーの維持が容易になります。共有オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

共有オブジェクトを調査する場合、Security Cloud Control ではオブジェクトの内容がオブジェクトテーブルに表示されます。共有オブジェクトの内容はまったく同じです。Security Cloud Control では、オブジェクトの要素の結合された、つまり「フラット化された」ビューが詳細ペインに表示されます。詳細ペインでは、ネットワーク要素が単純なリストにフラット化されており、名前付きオブジェクトに直接関連付けられていないことに注意してください。



オブジェクトのオーバーライド

オブジェクトのオーバーライドを使用すると、特定のデバイスの共有オブジェクトをカスタマイズできます。デバイスにオーバーライドがある場合、Security Cloud Control はオブジェクトのデフォルト値の代わりに、そのデバイスのオーバーライド値を使用します。

オーバーライドを使用すると、必要に応じて個々のオブジェクトの値を調整しながら、デバイス間で単一の共有ポリシーを維持できます。

たとえば、3 つのオフィスで共有しているプリントサーバーオブジェクトがあり、デフォルト値は 10.1.1.100 です。オフィス B には、10.2.1.100 に別のプリントサーバーがあります。個別のオブジェクトを作成する代わりに、値 10.2.1.100 のオフィス B のデバイスのオーバーライド

を追加します。オフィスBのデバイスはオーバーライドを使用します。他のすべてのデバイスはデフォルト値を使用します。

ネットワーク オブジェクト グループのオーバーライド

ネットワーク オブジェクト グループをオーバーライドすると、割り当てられているデバイスのデフォルト値が完全に置き換えられます。オーバーライド値を持つデバイスは、デフォルト値ではなく、オーバーライド値のみを受信します。これは、以下を意味します。

- デフォルト値への変更（追加、編集、または削除）は、オーバーライドされていないデバイスにのみ影響します。
- オーバーライド値を変更すると、その特定のオーバーライド値に割り当てられたデバイスにのみ影響します。

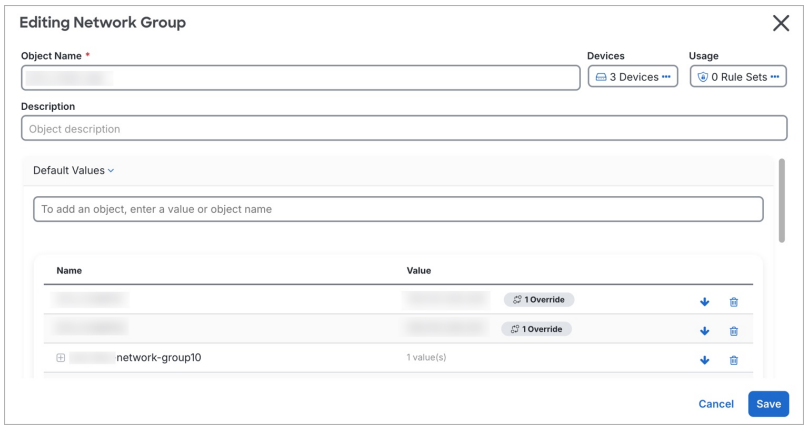
たとえば、3つのブランチオフィス（ブランチA、ブランチB、ブランチC）でファイアウォールを介して共有されているネットワークグループdns-serversがあるとします。このグループには、プライマリ dns（10.0.1.53）とセカンダリ dns（10.0.2.53）の 2 つのデフォルト値があります。ブランチCは、10.30.1.53でローカルDNSキャッシュも実行します。このキャッシュを含める必要があります。

ネットワークグループのオーバーライドによってデフォルトが完全に置き換えられるため、ブランチC のオーバーライドとして local-dns-cache のみを追加することはできません。これにより、ブランチ C のファイアウォールは local-dns-cache のみを受信し、プライマリ dns およびセカンダリ dns へのアクセスが失われます。代わりに、ブランチC のオーバーライドとして 3 つの値（プライマリ dns、セカンダリ dns、local-dns-cache）すべてを追加する必要があります。

この設定後、次が実行されます。

- ブランチ A およびブランチ B は、プライマリ dns、セカンダリ dns を受信します（デフォルト値から）。
- ブランチ C は、プライマリ dns、セカンダリ dns、local-dns-cache を受信します（オーバーライドから）。

後で新しいデフォルト値 tertiary-dns を追加すると、ブランチ A とブランチ B は自動的にそれを受信しますが、ブランチ C は受信しません。ブランチ C のオーバーライドにも tertiary-dns を追加する必要があります。



関連付けのないオブジェクト

ルールやポリシーですぐに使用するためのオブジェクトを作成できますが、ルールやポリシーに関連付けないオブジェクトを作成することもできます。関連付けられていないオブジェクトをルールまたはポリシーで使用すると、Security Cloud Control ではそのコピーが作成され、そのコピーが使用されます。関連付けられていない元のオブジェクトは、夜間のメンテナンスジョブで削除されるか、ユーザーが削除するまで、使用可能な一連のオブジェクト内に残ります。

関連付けられていないオブジェクトはコピーとして Security Cloud Control に残り、オブジェクトに関連付けられたルールまたはポリシーが誤って削除された場合にすべての設定が失われないようにします。

左側のペインで、[オブジェクト（Objects）] > [ ] の順にクリックし、[関連付けなし（Unassociated）] チェックボックスをオンにします。

オブジェクトの比較

手順

ステップ 1 左側のペインで、[オブジェクト（Objects）] をクリックして、オプションを選択します。

ステップ 2 ページのオブジェクトをフィルタ処理して、比較するオブジェクトを見つけます。

ステップ 3 [比較（Compare）] Compare ボタンをクリックします。

ステップ 4 比較するオブジェクトを最大 3 つまで選択します。

ステップ 5 画面の下部にオブジェクトを並べて表示します。

- [オブジェクトの詳細（Object Details）] タイトルバーの上下の矢印をクリックして、表示するオブジェクト詳細を調整します。

- [詳細（Details）] ボックスと [関係（Relationships）] ボックスを展開するか折りたたんで、表示する情報を調整します。

ステップ 6 （オプション）[関係（Relationships）] ボックスには、オブジェクトの使用方法が表示されます。オブジェクトはデバイスまたはポリシーに関連付けられている場合があります。オブジェクトがデバイスに関連付けられている場合は、デバイス名をクリックしてから [構成の表示（View Configuration）] をクリックして、デバイスの構成を表示できます。Security Cloud Control はデバイスの構成ファイルを表示し、そのオブジェクトのエントリをハイライトします。

フィルタ

[セキュリティデバイス（Security Devices）] ページと [オブジェクト（Objects）] ページのさまざまなフィルタを使用して、探しているデバイスやオブジェクトを検索できます。

フィルタ処理するには、[セキュリティデバイス（Security Devices）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト（Objects）] タブの左側のペインで  をクリックします。

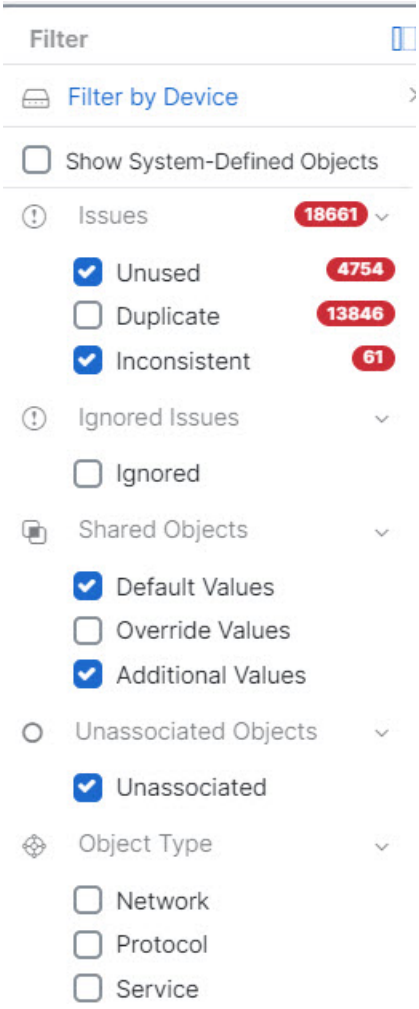
セキュリティ デバイス フィルタでは、デバイスタイプ、ハードウェアとソフトウェアのバージョン、Snort バージョン、設定ステータス、接続状態、競合検出、Secure Device Connector、およびラベルでフィルタ処理できます。フィルタを適用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。フィルタを使用して、選択したデバイスタイプのタブ内のデバイスを見つけることができます。

オブジェクトフィルタを使用すると、デバイス、問題タイプ、共有オブジェクト、関連付けのないオブジェクト、およびオブジェクトタイプでフィルタ処理できます。結果にシステムオブジェクトを含めるかどうかを選択できます。検索フィールドを使用して、特定の名前、IP アドレス、またはポート番号を含むフィルタ結果内のオブジェクトを検索することもできます。

オブジェクトタイプフィルタを使用すると、ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなどのタイプによってオブジェクトをフィルタ処理できます。共有オブジェクトフィルタを使用すると、デフォルト値またはオーバーライド値を持つオブジェクトをフィルタ処理できます。

デバイスとオブジェクトをフィルタ処理する場合、検索語を組み合わせて、関連する結果を見つけるためのいくつかの潜在的な検索戦略を作成することができます。

次の例では、「問題（使用されていない、または、不整合）、かつ、共有オブジェクト（デフォルト値、または、追加の値を持つ）かつ、関連付けられていないオブジェクト」を検索するフィルタが適用されます。



オブジェクトフィルタ

フィルタ処理するには、[オブジェクト（Object）] タブの左側のペインで をクリックします。

- [デバイスごとのフィルタ（Filter by Device）]：特定のデバイスを選択して、選択したデバイスで見つかったオブジェクトを表示できます。
- [問題（Issues）]：未使用のオブジェクト、重複するオブジェクト、および一貫性のないオブジェクトを選択して表示できます。
- [無視された問題（Ignored Issues）]：不整合を無視したすべてのオブジェクトを表示できます。
- [共有オブジェクト（Shared Objects）]：複数のデバイスで共有されていることが Security Cloud Control によって検出されたすべてのオブジェクトを表示できます。デフォルト値またはオーバーライド値のみ、あるいはその両方を持つ共有オブジェクトを表示することを選択できます。

- [関連付けられていないオブジェクト（Unassociated Objects）]：ルールまたはポリシーに関連付けられていないすべてのオブジェクトを表示できます。
- [オブジェクトタイプ（Object Type）]：オブジェクトタイプを選択して、ネットワークオブジェクト、ネットワークグループ、URL オブジェクト、URL グループ、サービスオブジェクト、サービスグループなど、選択したタイプのオブジェクトのみを表示できます。

サブフィルタ–各メインフィルタ内には、選択をさらに絞り込むために適用できるサブフィルタがあります。これらのサブフィルタは、オブジェクトタイプ（ネットワーク、サービス、プロトコルなど）に基づいています。

このフィルタバーで選択されたフィルタは、以下の条件に一致するオブジェクトを返します。

*****2つのデバイスのいずれかにあるオブジェクト（[デバイスでフィルタ処理（Filter by Device）]をクリックしてデバイスを指定します）。および

*** 一貫性のない**オブジェクト。および

*** ネットワーク**オブジェクトまたは**サービス**オブジェクト。 および

***** オブジェクトの命名規則に「**グループ**」という単語が含まれているオブジェクト。

[システムオブジェクトの表示（Show System Objects）] がオンになっているため、結果にはシステムオブジェクトとユーザー定義オブジェクトの両方が含まれます。

[システム定義オブジェクトの表示（Show System-Defined Objects）] フィルタ

一部のデバイスには、一般的なサービス用に事前定義されたオブジェクトがあります。これらのシステム オブジェクトは既に作成されており、ルールやポリシーで使用できるので便利です。オブジェクトテーブルには多くのシステムオブジェクトが含まれる場合があります。システムオブジェクトは編集または削除できません。

[システム定義オブジェクトの表示（Show System-Defined Objects）]は、デフォルトでは**オフ**になっています。オブジェクトテーブルにシステムオブジェクトを表示するには、フィルタバーで [システム定義オブジェクトの表示（Show System-Defined Objects）] をオンにします。オブジェクトテーブルでシステムオブジェクトを非表示にするには、フィルタバーで [システムオブジェクトを表示（Show System Objects）] をオフのままにします。

システムオブジェクトを非表示にすると、それらは検索およびフィルタ処理の結果に含まれなくなります。システムオブジェクトを表示すると、それらはオブジェクトの検索とフィルタ処理の結果に含まれます。

オブジェクトフィルタを設定する

条件を必要な数だけ設定してフィルタリングできます。フィルタリングするカテゴリが多いほど、予想される結果は少なくなります。

手順

ステップ 1　左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 2 ページ上部のフィルタアイコン  をクリックして、フィルタパネルを開きます。オブジェクトが誤って除外されないように、チェック付きのフィルタのチェックを外します。さらに、検索フィールドを見て、検索フィールドに入力された可能性のあるテキストを削除します。

ステップ 3 結果を特定のデバイスで見つかったものに限定したい場合：

1. **[デバイスでフィルタ処理（Filter By Device）]** をクリックします。
2. すべてのデバイスを検索するか、デバイスタブをクリックして特定の種類のデバイスのみを検索します。
3. フィルタ条件に含めるデバイスのチェックボックスをオンにします。
4. [OK] をクリックします。

ステップ 4 検索結果にシステムオブジェクトを含めるには、[システムオブジェクトを表示（Show System Objects）] をオンにします。検索結果でシステムオブジェクトを除外するには、[システムオブジェクトを表示（Show System Objects）] をオフにします。

ステップ 5 [問題（Issues）] で、フィルタリングするオブジェクトの問題のチェックボックスをオンにします。複数の問題をオンにすると、オンにしたいずれかのカテゴリのオブジェクトがフィルタ結果に含まれます。

ステップ 6 問題があったが管理者によって無視されたオブジェクトを表示する場合は、[無視（Ignored）] の問題をチェックします。

ステップ 7 2つ以上のデバイス間で共有されるオブジェクトをフィルタリングする場合は、[共有オブジェクト（Shared Objects）] で必要なフィルタをオンにします。

- [デフォルト値（Default Values）]：デフォルト値のみを持つオブジェクトをフィルタリングします。
- [オーバーライド値（Override Values）]：オーバーライドされた値を持つオブジェクトをフィルタリングします。
- [追加の値（Additional Values）]：追加の値を持つオブジェクトをフィルタリングします。

ステップ 8 ルールまたはポリシーの一部ではないオブジェクトをフィルタリングする場合は、[関連付けなし（Unassociated）] をオンにします。

ステップ 9 フィルタリングする [オブジェクトタイプ（Object Types）] をオンにします。

ステップ 10 オブジェクト名、IP アドレス、またはポート番号を [オブジェクト（Objects）] 検索フィールドに追加して、フィルタリングされた結果の中から検索条件に一致するオブジェクトを見つけることもできます。

フィルタ基準からデバイスを除外する場合

デバイスをフィルタリング基準に追加すると、結果にはデバイス上のオブジェクトは表示されますが、それらのオブジェクトと他のデバイスとの関係は表示されません。たとえば、**ObjectA** が ASA1 と ASA2 の間で共有されている場合、オブジェクトをフィルタリングして ASA1 上の共有オブジェクトを検索すると、**ObjectA** は見つかりますが、[関係（Relationships）] ペインには、オブジェクトが ASA1 にあることだけが表示されます。

オブジェクトが関連するすべてのデバイスを表示するには、検索条件でデバイスを指定しないでください。他の条件でフィルタリングし、必要に応じて検索条件を追加します。Security Cloud Control が識別するオブジェクトを選択し、[関係（Relationships）] ペインを調べます。そのオブジェクトに関連するすべてのデバイスとポリシーが表示されます。

オブジェクトの無視の解除

未使用、重複、不整合のオブジェクトを解決する方法の 1 つは、それらを無視することです。オブジェクトが未使用、重複、または不整合であっても、その状態には正当な理由があると判断し、オブジェクトの問題を未解決のままにすることを選択する場合もあります。将来のある時点で、これらの無視されたオブジェクトを解決することが必要になる場合があります。オブジェクトの問題を検索するときに Security Cloud Control は無視されたオブジェクトを表示しないため、無視されたオブジェクトのオブジェクトリストをフィルタリングし、結果に基づいて操作する必要があります。

手順

ステップ 1 左側のペインで、[オブジェクト（Objects）] をクリックして、オプションを選択します。

ステップ 2 無視されたオブジェクトをフィルタリングして検索します。

ステップ 3 [オブジェクト（Object）]テーブルで、無視を解除するオブジェクトをすべて選択します。一度に 1 つのオブジェクトの無視を解除できます。

ステップ 4 詳細ペインで [無視の解除（Unignore）] をクリックします。

ステップ 5 要求を確認します。これで、オブジェクトを問題でフィルタリングすると、以前は無視されていたオブジェクトが見つかるはずです。

オブジェクトの削除

1 つのオブジェクトまたは複数のオブジェクトを削除できます。

1 つのオブジェクトの削除

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、およびFTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで [オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、削除するオブジェクトを見つけ、それを選択します。

ステップ 3 [関係（Relationships）] ペインを確認します。オブジェクトがポリシーまたはオブジェクトグループで使用されている場合は、そのポリシーまたはグループから削除するまでオブジェクトを削除できません。

ステップ 4 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。

ステップ 5 [OK] をクリックしてオブジェクトの削除を確認します。

ステップ 6 行った変更をレビューして展開するか、待機してから複数の変更を一度に展開します。

未使用オブジェクトのグループの削除

デバイスをオンボードしてオブジェクトの問題解決に取り組むと、多くの未使用のオブジェクトが見つかります。一度に最大 50 個の未使用オブジェクトを削除できます。

手順

ステップ 1 [問題（Issues）] フィルタを使用して、**未使用のオブジェクト**を見つけます。デバイスフィルタを使用する際に [デバイスなし（No Device）] を選択し、デバイスに関連付けられていないオブジェクトを検索することもできます。オブジェクトリストをフィルタリングすると、オブジェクトのチェックボックスが表示されます。

ステップ 2 オブジェクト テーブル ヘッダーの [すべて選択（Select all）] チェックボックスをオンにして、フィルタによって検出されオブジェクトテーブルに表示されるすべてのオブジェクトを選択するか、削除する個々のオブジェクトの個々のチェックボックスをオンにします。

ステップ 3 [アクション（Actions）] ペインで、[削除（Remove）] アイコン をクリックします。

ステップ 4 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

ネットワーク オブジェクト

1 つのネットワークオブジェクトには、ホスト名、ネットワーク IP アドレス、IP アドレスの範囲、完全修飾ドメイン名（FQDN）または CIDR 表記のサブネットワークのいずれか 1 つを入れることができます。[ネットワークグループ（Network groups）] は、ネットワークオブジェクトと、グループに追加するその他の個々のアドレスまたはサブネットワークのコレクションです。ネットワークオブジェクトとネットワークグループは、アクセスルール、ネットワークポリシー、および NAT ルールで使用されます。

すべてのプラットフォームが Cisco Meraki や Multicloud Defense などのネットワークオブジェクトをサポートしているわけではないことに注意してください。ダイナミックオブジェクトを共有すると、Security Cloud Control は、発信元のプラットフォームまたはデバイスからの適切な情報を、Security Cloud Control が使用できる一連の使用可能な情報に自動的に変換します。

製品間でのネットワークオブジェクトの再利用

クラウド提供型 Firewall Management Center とテナントにオンボーディングされている 1 つ以上の オンプレミス Firewall Management Center を含む Security Cloud Control テナントがある場合は、次の手順を実行します。

- Cisco Secure Firewall Threat Defense、FDM による管理Firewall Threat Defense、Cisco ASA、または Cisco Meraki ネットワークオブジェクトまたはグループを作成すると、そのオブジェクトのコピーが、クラウド提供型 Firewall Management Center の設定時に使用する [オブジェクト（Objects）] ページのオブジェクトリストにも追加されます。その逆も同様です。

- Cisco Secure Firewall Threat Defense、FDM による管理Firewall Threat Defense、または ASA ネットワークオブジェクトまたはグループを作成すると、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている各オンプレミス Firewall Management Center の [保留中の変更があるデバイス（Devices with Pending Changes）] ページにエントリが作成されます。このリストから、オブジェクトを選択して、そのオブジェクトを使用するオンプレミス Firewall Management Center に展開し、不要なオブジェクトを破棄できます。、**[管理（Administration）] > [Firewall Management Center]** に移動しオンプレミス Firewall Management Center を選択します。[オブジェクト（Objects）] をクリックし、オンプレミス Firewall Management Center ユーザーインターフェイスでオブジェクトを確認して、ポリシーに割り当てます。

いずれかのページのネットワークオブジェクトやグループに加えた変更は、両方のページのオブジェクトまたはグループインスタンスに適用されます。1 つのページからオブジェクトを削除すると、そのオブジェクトの対応するコピーも他のページから削除されます。

例外：

- 同じ名前のネットワークオブジェクトがすでにクラウド提供型 Firewall Management Center に存在する場合、新しい Cisco Secure Firewall Threat Defense、FDM による管理 Firewall Threat Defense、Cisco ASA、または Cisco Meraki ネットワークオブジェクトは、Security Cloud Control の [オブジェクト（Objects）] ページには複製されません。
- オンプレミスの Cisco Secure Firewall Management Center によって管理されるオンボード済み Firewall Threat Defense デバイスのネットワークオブジェクトおよびグループは複製されず、クラウド提供型 Firewall Management Center で使用できません。

  クラウド提供型 Firewall Management Center に移行したオンプレミスの Cisco Secure Firewall Management Center インスタンスの場合、ネットワークオブジェクトとグループは、FTD デバイスに展開されたポリシーで使用されていれば、Security Cloud Control オブジェクトページに複製されることに注意してください。
- Security Cloud Control と クラウド提供型 Firewall Management Center の間のネットワークオブジェクトの共有は、新しいテナントでは自動的に有効になりますが、既存のテナントでは要求する必要があります。ネットワークオブジェクトが クラウド提供型 Firewall Management Center と共有されていない場合は、TAC に連絡して、テナントで機能を有効にしてもらいます。
- Security Cloud Control とオンプレミス Firewall Management Center の間のネットワークオブジェクトの共有は、Security Cloud Control に対して導入準備された新しいオンプレミス Firewall Management Center の Security Cloud Control では自動的に有効になりません。ネットワークオブジェクトがオンプレミス Firewall Management Center と共有されていない場合は、[設定（Settings）] でオンプレミス Firewall Management Center の [ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルボタンが有効になっていることを確認するか、TAC に連絡してテナントで機能を有効にしてもらいます。

ネットワークオブジェクトの表示

Security Cloud Control を使用して作成するネットワークオブジェクトと、オンボーディングしたデバイスの設定から Security Cloud Control が認識するネットワークオブジェクトは、[オブジェクト（Objects）] ページに表示されます。これらのネットワークオブジェクトには、それぞれのオブジェクトタイプのラベルが付けられています。これにより、オブジェクトタイプでフィルタリングして、探しているオブジェクトをすばやく見つけることができます。

[オブジェクト（Objects）]ページでネットワークオブジェクトを選択すると、オブジェクトの値が [詳細（Detail）] ペインに表示されます。[関係（Relationships）] ペインには、オブジェクトがポリシーで使用されているかどうか、およびオブジェクトが保存されているデバイスが表示されます。

ネットワークグループをクリックすると、そのグループの内容が表示されます。ネットワークグループは、ネットワークオブジェクトによってグループに与えられたすべての値の集合体です。

ASA ネットワークオブジェクトおよびネットワークグループの作成または編集

ASA ネットワークオブジェクトには、CIDR 表記で表現されたホスト名、IP アドレス、またはサブネットアドレスを含めることができます。**ネットワークグループ**は、アクセスルール、ネットワークポリシー、および NAT ルールで使用されるネットワークオブジェクト、ネットワークグループ、および IP アドレスの集合体です。Security Cloud Control を使用して、ネットワークオブジェクトとネットワークグループを作成、読み取り、更新、および削除できます。

表 *3 : ASA* ネットワークオブジェクトおよびグループで許可される値

デバイス タイプ（**Device Type**）	**[IPv4 / IPv6]**	シングル アドレス	アドレス範囲	部分修飾ドメイン名（**PQDN**）	**CIDR** 表記法によるサブネット
ASA	[IPv4 / IPv6]	対応	対応	対応	対応

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

ASA ネットワークオブジェクトの作成

1 つのネットワークオブジェクトには、ホスト名、ネットワーク IP アドレス、IP アドレスの範囲、完全修飾ドメイン名（FQDN）または CIDR 表記のサブネットワークのいずれか 1 つを入れることができます。ネットワークオブジェクトは、アクセスルール、ネットワークポリ

シー、およびNAT ルールで使用されます。Security Cloud Control を使用して、ネットワークオブジェクトとネットワークグループを作成、更新、および削除できます。

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）]ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Centerに自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[ASA]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 オブジェクト名を入力します。

ステップ 5 [ネットワークオブジェクトの作成（Create a network object）] を選択します。

ステップ 6 （任意）オブジェクトの説明を入力します。

ステップ 7 [値（Value）] セクションで、次のいずれかの方法で IP アドレス情報を追加します。

- [eq] を選択し、単一の IP アドレス、CIDR 表記を使用したサブネットアドレス、または部分修飾ドメイン名（PQDN）を入力します。
- [範囲（range）] を選択し、IP アドレスの範囲を入力します。範囲の開始アドレスと終了アドレスをスペースで区切って入力します。例：10.1.1.1 10.1.1.255 または 2001:DB8:1::1 2001:DB8:1::3

ステップ 8 [追加（Add）] をクリックします。

重要
新たに作成されたネットワークオブジェクトは、ルールやポリシーの一部ではないため、いずれのASAデバイスにも関連付けられていません。それらのオブジェクトを表示するには、オブジェクトフィルタで[関連付けなし（Unassociated）] オブジェクトカテゴリを選択します。

詳細については、「オブジェクトフィルタ」を参照してください。デバイスのルールやポリシーに関連付けられていないオブジェクトを使用すると、そのオブジェクトはそのデバイスに関連付けられます。

ASA ネットワーク グループの作成

[ネットワークグループ（network group）] には、IP アドレス値、ネットワークオブジェクト、およびネットワークグループを含めることができます。新しいネットワークグループを作成するときに、名前、IP アドレス、IP アドレス範囲、または FQDN で既存のオブジェクトを検索し、[ネットワークグループ（network group）] に追加できます。オブジェクトが存在しない場合は、同じインターフェイスでそのオブジェクトをすぐに作成し、[ネットワークグループ（Network Group）] に追加できます。ネットワークグループには、IPv4 と IPv6 の両方のアドレスを含めることができます。

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 青色のプラスボタン  をクリックして、オブジェクトを作成します。

ステップ 3 **[ASA]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 [ネットワークグループの作成（Create a network group）] を選択します。

ステップ 6 （任意）オブジェクトの説明を入力します。

ステップ 7 [値（Values）] フィールドに、値またはオブジェクト名を入力します。入力を開始すると、入力に一致するオブジェクト名または値が Security Cloud Control によって表示されます。

ステップ 8 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 9 Security Cloud Control で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。

ステップ 10 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

（注）
編集アイコンをクリックして、詳細を変更できます。削除ボタンをクリックしても、オブジェクト自体は削除されず、代わりに、ネットワークグループから削除されます。

ステップ 11 必要なオブジェクトを追加したら、[追加（Add）] をクリックして新しいネットワークグループを作成します。

ステップ 12 すべてのデバイスの設定変更のプレビューと展開。

ASA ネットワークオブジェクトの編集

⚠

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 3 ネットワークオブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 ダイアログボックスの値を、上記の手順で作成したときと同じ方法で編集します。

（注）
ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。

ステップ 6 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ASA ネットワークグループの編集

⚠

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと [検索（Search）] フィールドを使用して、編集するネットワークグループを見つけます。

ステップ 3 ネットワークグループを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 ネットワークグループにすでに追加されているオブジェクトまたはネットワークグループを変更する場合は、次の手順を実行します。

1. オブジェクト名またはネットワークグループの横に表示される編集アイコン をクリックして、それらを変更します。
2. チェックマークをクリックして変更内容を保存します。

（注）
削除アイコンをクリックして、ネットワークグループから値を削除できます。

ステップ 5 ネットワークグループに新しいネットワークオブジェクトまたはネットワークグループを追加する場合は、次の手順を実行する必要があります。

1. [値（Values）] フィールドに、新しい値または既存のネットワークオブジェクトの名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が Security Cloud Control によって表示されます。表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。
2. Security Cloud Control で一致が検出された場合、既存のオブジェクトを選択するには、**[Add]** をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。
3. 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。
   - [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
   - [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
   - [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 6 [保存（Save）] をクリックします。Security Cloud Control に変更の影響を受けるポリシーが表示されます。

ステップ 7 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 8 すべてのデバイスの設定変更のプレビューと展開。

Security Cloud Control における共有ネットワークグループへの追加の値の追加

関連付けられているすべてのデバイスに存在する共有ネットワークグループの値は、「デフォルト値」と呼ばれます。Security Cloud Control を使用すると、共有ネットワークグループに「追加の値」を追加し、その共有ネットワークグループに関連付けられている一部のデバイスにそれらの値を割り当てることができます。Security Cloud Control がデバイスに変更を展開するときに、内容が決定され、「デフォルト値」が共有ネットワークグループに関連付けられているすべてのデバイスにプッシュされ、「追加の値」が指定されたデバイスにのみプッシュされます。

たとえば、本社に 4 つの AD メインサーバーがあり、すべての拠点からアクセスできる必要があるシナリオを考えてみます。この状況で、すべての拠点で使用する「Active-Directory」という名前のオブジェクトグループを作成しました。ここで、ブランチオフィスの 1 つにさらに 2 つの AD サーバーを追加します。これを行うには、オブジェクトグループ「Active-Directory」で、分散拠点に固有の追加値として詳細を追加します。これら 2 つのサーバーは、オブジェクト「Active-Directory」が一貫しているか、または共有されているかの判断には関与しません。したがって、4 つの AD メインサーバーはすべての拠点からアクセスできますが、ブランチオ

フィス（2 つの追加サーバーがある）は 2 つの AD サーバーと 4 つの AD メインサーバーにアクセスできます。

（注） 一貫性のない共有ネットワークグループがある場合は、追加の値を使用してそれらを 1 つの共有ネットワークグループに結合できます。詳細については、「不整合オブジェクトの問題を解決する」を参照してください。

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集する共有ネットワークグループを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

- [Device）] フィールドには、共有ネットワークグループが存在するデバイスが表示されます。
- [使用（Usage）] フィールドには、共有ネットワークグループに関連付けられたルールセットが表示されます。
- [デフォルト値] フィールドは、デフォルトのネットワークオブジェクトと、オブジェクトの作成時に指定された、共有ネットワークグループに関連付けられたオブジェクト値が示されます。このフィールドの横に、このデフォルト値を含むデバイスの数が表示され、クリックすると名前とデバイスタイプを表示できます。この値に関連付けられたルールセットも表示されます。

ステップ 4 [追加の値（Additional Values）] フィールドに、値または名前を入力します。 入力を開始すると、入力に一致するオブジェクト名または値が Security Cloud Control によって表示されます。

ステップ 5 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 6 Security Cloud Control で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。

ステップ 7 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。
- [値の追加（Add Value）] をクリックして、オブジェクトを使用せずにインライン値を作成します。値を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 8 [デバイス（Devices）] 列で、新しく追加されたオブジェクトに関連付けられているセルをクリックし、[デバイスの追加（Add Devices）] をクリックします。

ステップ 9 必要なデバイスを選択し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。

ステップ 11 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 12 すべてのデバイスの設定変更のプレビューと展開。

Security Cloud Control における共有ネットワークグループの追加の値の編集

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [デバイス（Devices）] 列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [デフォルト値（Default Values）] の 矢印をクリックすると、共有ネットワークグループの追加値にできます。共有ネットワークグループに関連付けられているすべてのデバイスが、自動的に割り当てられます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有ネットワークグループのデフォルト値にできます。
- ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。

ステップ 6 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 7 すべてのデバイスの設定変更のプレビューと展開。

Security Cloud Control のネットワークオブジェクトとグループの削除

クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

オブジェクト ページからネットワークオブジェクトまたはグループを削除すると、クラウド提供型 Firewall Management Center の **オブジェクト** ページから重複するネットワークオブジェクトまたはグループが削除されます。その逆も同様です。

Firepower ネットワークオブジェクトまたはネットワークグループの作成または編集

Firepower ネットワークオブジェクトには、CIDR 表記で表現されたホスト名、IP アドレス、またはサブネットアドレスを含めることができます。**ネットワークグループ**は、アクセスルール、ネットワークポリシー、およびNATルールで使用されるネットワークオブジェクトとネットワークグループの集合体です。Security Cloud Control を使用して、ネットワークオブジェクトとネットワークグループを作成、読み取り、更新、および削除できます。

Firepower ネットワークオブジェクトおよびグループは、ASA、Firewall Threat Defense、FDM による管理、および Meraki デバイスで使用できます。「製品間でのネットワークオブジェクトの再利用 （35 ページ）」を参照してください。

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

表 *4:* ネットワークオブジェクトに追加できる *IP* アドレス

デバイス タイプ（Device Type）	[IPv4 / IPv6]	シングル アドレス	アドレス範囲	部分修飾ドメイン名（PQDN）	CIDR 表記法によるサブネット
Firepower	[IPv4 / IPv6]	対応	対応	対応	対応

関連情報

- Firepower ネットワークオブジェクトの作成 （47 ページ）
- Firepower ネットワークオブジェクトの編集 （49 ページ）
- 共有ネットワークグループへの追加の値の追加 （53 ページ）
- 共有ネットワークグループの追加の値の編集 （55 ページ）

Firepower ネットワークオブジェクトの作成

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーがクラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 青色のプラスボタン をクリックして、オブジェクトを作成します。

ステップ 3 **[FTD]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 [ネットワークオブジェクトの作成（Create a network object）] を選択します。

ステップ 6 [値（Value）] セクションで、次の手順を実行します。

- [eq] を選択し、単一の IP アドレス、CIDR 表記で表されるサブネットアドレス、または部分修飾ドメイン名（PQDN）を入力します。
- [範囲（range）] を選択し、IP アドレスの範囲を入力します。

（注）
ホストビット値を設定しないでください。0 以外のホストビット値を入力すると、オブジェクトの作成中に Security Cloud Control が設定を解除します。これは、クラウド提供型 Firewall Management Center はホストビットが設定されていない IPv6 オブジェクトのみを受け入れるためです。

ステップ 7 [Add] をクリックします。

[Attention（注意）]：新たに作成されたネットワークオブジェクトは、ルールやポリシーの一部ではないため、いずれの FDM による管理 デバイスにも関連付けられていません。それらのオブジェクトを表示するには、オブジェクトフィルタで [関連付けなし（Unassociated）] オブジェクトカテゴリを選択します。詳細については、「オブジェクトフィルタ」を参照してください。デバイスのルールやポリシーに関連付けられていないオブジェクトを使用すると、そのオブジェクトはそのデバイスに関連付けられます。

Firepower ネットワークグループの作成

[ネットワークグループ（network group）] には、ネットワークオブジェクトとネットワークグループを含めることができます。新しいネットワークグループを作成するときに、名前、IP アドレス、IP アドレス範囲、または FQDN で既存のオブジェクトを検索し、[ネットワークグループ（network group）] に追加できます。オブジェクトが存在しない場合は、同じインターフェイスでそのオブジェクトをすぐに作成し、[ネットワークグループ（Network Group）] に追加できます。

（注） クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

FTD、FDM、または Cisco ASA ネットワークオブジェクトやグループを [オブジェクト（Objects）] ページで作成すると、オブジェクトのコピーが クラウド提供型 Firewall Management Center に自動的に追加されます。その逆も同様です。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリからオブジェクトを選択し、それらのオブジェクトを必要とする オンプレミス Firewall Management Center に展開できます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 青色のプラスボタン をクリックして、オブジェクトを作成します。

ステップ 3 **[FTD]** > **[ネットワーク（Network）]** をクリックします。

ステップ 4 [オブジェクト名（Object Name）] を入力します。

ステップ 5 [ネットワークグループの作成（Create a network group）] を選択します。

ステップ 6 [値（Values）] フィールドに、値または名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が Security Cloud Control によって表示されます。

ステップ 7 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 8 Security Cloud Control で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。

ステップ 9 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

注：編集アイコンをクリックして、詳細を変更できます。削除ボタンをクリックしても、オブジェクト自体は削除されず、代わりに、ネットワークグループから削除されます。

ステップ 10 必要なオブジェクトを追加したら、[保存（Save）] をクリックして新しいネットワークグループを作成します。

ステップ 11 すべてのデバイスの設定変更をプレビューして展開します。

Firepower ネットワークオブジェクトの編集

⚠

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集するオブジェクトを見つけます。

ステップ 3 ネットワークオブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 「Firepower ネットワークグループの作成」で作成したのと同じ方法で、ダイアログボックスの値を編集します。

（注）
ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。

ステップ 6 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

Firepower ネットワークグループの編集

⚠

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、およびFTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと [検索（Search）] フィールドを使用して、編集するネットワークグループを見つけます。

ステップ 3 ネットワークグループを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 オブジェクトの名前と説明を必要に応じて変更します。

ステップ 5 ネットワークグループにすでに追加されているオブジェクトまたはネットワークグループを変更する場合は、次の手順を実行します。

1. オブジェクト名またはネットワークグループの横に表示される編集アイコン をクリックして、それらを変更します。
2. チェックマークをクリックして変更内容を保存します。**注**：削除アイコンをクリックして、ネットワークグループから値を削除できます。

ステップ 6 ネットワークグループに新しいネットワークオブジェクトまたはネットワークグループを追加する場合は、次の手順を実行する必要があります。

1. [値（Values）] フィールドに、新しい値または既存のネットワークオブジェクトの名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が Security Cloud Control によって表示されます。表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。
2. Security Cloud Control で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。
3. 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 7 [保存（Save）] をクリックします。Security Cloud Control に変更の影響を受けるポリシーが表示されます。

ステップ 8 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 9 すべてのデバイスの設定変更をプレビューして展開します。

オブジェクトオーバーライドの追加

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、およびFTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、オーバーライドを追加するオブジェクトを見つけます。

ステップ 3 ネットワークオブジェクトを選択し、[アクション（Actions）] ペインで編集アイコン をクリックします。

ステップ 4 [オーバーライド値（Override Values）] ダイアログボックスに値を入力し、[+ 値の追加（+ Add Value）] をクリックします。

重要

追加するオーバーライドは、オブジェクトに含まれる値と同じ型である必要があります。たとえば、ネットワークオブジェクトに対しては、ホスト値ではなくネットワーク値のみでオーバーライドを構成できます。

ステップ 5 値が追加されたことを確認したら、[オーバーライド値（Override Values）] の [デバイス（Devices）] 列でセルをクリックします。

ステップ 6 [デバイスの追加（Add Devices）] をクリックし、オーバーライドを追加するデバイスを選択します。選択するデバイスには、オーバーライドを追加するオブジェクトが含まれている必要があります。

ステップ 7 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。

ステップ 8 [確認（Confirm）]をクリックして、オブジェクトとその影響を受けるデバイスへのオーバーライドの追加を確定します。

（注）
1つのオブジェクトに複数のオーバーライドを追加できます。ただし、オーバーライドを追加するたびに、オブジェクトを含む別のデバイスを選択する必要があります。

ステップ 9 オブジェクトオーバーライドの詳細については「オブジェクトのオーバーライド （26 ページ）」を、既存のオーバーライドの編集については「オブジェクトオーバーライドの編集 （52 ページ）」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

オブジェクトがデバイスに存在している間は、既存のオーバーライドの値を変更できます。

手順

ステップ 1 **オブジェクト** にアクセスします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 オーバーライドがあるオブジェクトを選択し、[アクション（Actions）]ペインで編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [オーバーライド値（Override Values）] で [デバイス（Devices）] 列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有オブジェクトのデフォルト値にできます。
- 削除するオーバーライドの横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。
ステップ 6 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。
ステップ 7 すべてのデバイスの設定変更をプレビューして展開します。

共有ネットワークグループへの追加の値の追加

関連付けられているすべてのデバイスに存在する共有ネットワークグループの値は、「デフォルト値」と呼ばれます。Security Cloud Control を使用すると、共有ネットワークグループに「追加の値」を追加し、その共有ネットワークグループに関連付けられている一部のデバイスにそれらの値を割り当てることができます。Security Cloud Control がデバイスに変更を展開するときに、内容が決定され、「デフォルト値」が共有ネットワークグループに関連付けられているすべてのデバイスにプッシュされ、「追加の値」が指定されたデバイスにのみプッシュされます。

たとえば、本社に 4 つの AD メインサーバーがあり、すべての拠点からアクセスできる必要があるシナリオを考えてみます。この状況で、すべての拠点で使用する「Active-Directory」という名前のオブジェクトグループを作成しました。ここで、ブランチオフィスの 1 つにさらに 2 つの AD サーバーを追加します。これを行うには、オブジェクトグループ「Active-Directory」で、分散拠点に固有の追加値として詳細を追加します。これら 2 つのサーバーは、オブジェクト「Active-Directory」が一貫しているか、または共有されているかの判断には関与しません。したがって、4 つの AD メインサーバーはすべての拠点からアクセスできますが、ブランチオフィス（2 つの追加サーバーがある）は 2 つの AD サーバーと 4 つの AD メインサーバーにアクセスできます。

（注） 一貫性のない共有ネットワークグループがある場合は、追加の値を使用してそれらを 1 つの共有ネットワークグループに結合できます。詳細については、不整合オブジェクトの問題を解決するを参照してください。

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、および FTD ネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集する共有ネットワークグループを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

- [デバイス（Devices）] フィールドには、共有ネットワークグループが存在するデバイスが表示されます。
- [使用（Usage）] フィールドには、共有ネットワークグループに関連付けられたルールセットが表示されます。
- [デフォルト値] フィールドは、デフォルトのネットワークオブジェクトと、オブジェクトの作成時に指定された、共有ネットワークグループに関連付けられたオブジェクト値が示されます。このフィールドの横に、このデフォルト値を含むデバイスの数が表示され、クリックすると名前とデバイスタイプを表示できます。この値に関連付けられたルールセットも表示されます。

ステップ 4 [追加の値（Additional Values）] フィールドに、値または名前を入力します。入力を開始すると、入力に一致するオブジェクト名または値が Security Cloud Control によって表示されます。

ステップ 5 表示されている既存のオブジェクトの 1 つを選択するか、入力した名前または値に基づいて新しいオブジェクトを作成できます。

ステップ 6 Security Cloud Control で一致が検出された場合、既存のオブジェクトを選択するには、[追加（Add）] をクリックして、ネットワークオブジェクトまたはネットワークグループを新しいネットワークグループに追加します。

ステップ 7 存在しない値またはオブジェクトを入力した場合は、次のいずれかを実行できます。

- [この名前の新しいオブジェクトとして追加（Add as New Object With This Name）] をクリックして、その名前の新しいオブジェクトを作成します。値を入力し、チェックマークをクリックして保存します。
- [新しいオブジェクトの追加（Add as New Object）] をクリックして、新しいオブジェクトを作成します。オブジェクト名と値は同じです。名前を入力し、チェックマークをクリックして保存します。

値がすでに存在していても、新しいオブジェクトは作成できます。それらのオブジェクトに変更を加えて保存できます。

ステップ 8 [デバイス（Devices）] 列で、新しく追加されたオブジェクトに関連付けられているセルをクリックし、[デバイスの追加（Add Devices）] をクリックします。

ステップ 9 必要なデバイスを選択し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。

ステップ 11 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 12 すべてのデバイスの設定変更をプレビューして展開します。

共有ネットワークグループの追加の値の編集

注意 クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

Cisco ASA、FDM、およびFTDネットワークオブジェクトやグループに加えた変更は、対応する クラウド提供型 Firewall Management Center ネットワークオブジェクトやグループに反映されます。さらに、[変更が保留中のデバイス（Devices with Pending Changes）] ページには、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている オンプレミス Firewall Management Center ごとにエントリが作成されます。このエントリから変更を選択し、それらのオブジェクトがある オンプレミス Firewall Management Center に展開できます。

いずれかのページからネットワークオブジェクトまたはグループを削除すると、両方のページからそのオブジェクトまたはグループは削除されます。

手順

ステップ 1 左側のペインで **オブジェクト** をクリックします。

ステップ 2 オブジェクトフィルタと検索フィールドを使用して、編集対象のオーバーライドがあるオブジェクトを見つけます。

ステップ 3 [アクション（Actions）] ペインにある編集アイコン をクリックします。

ステップ 4 オーバーライド値を変更します。

- 値を変更するには、編集アイコンをクリックします。
- [デバイス（Devices）] 列のセルをクリックして、新しいデバイスを割り当てます。すでに割り当てられているデバイスを選択し、[オーバーライドの削除（Remove Overrides）] をクリックすると、そのデバイスのオーバーライドを削除できます。
- [デフォルト値（Default Values）] の 矢印をクリックすると、共有ネットワークグループの追加値にできます。共有ネットワークグループに関連付けられているすべてのデバイスが、自動的に割り当てられます。
- [オーバーライド値（Override Values）] の 矢印をクリックすると、共有ネットワークグループのデフォルト値にできます。
- ネットワークグループからオブジェクトを削除するには、横にある削除アイコンをクリックします。

ステップ 5 [保存（Save）] をクリックします。Security Cloud Control は、変更の影響を受けるデバイスを表示します。

ステップ 6 [確認（Confirm）] をクリックして、オブジェクトとその影響を受けるデバイスへの変更を確定します。

ステップ 7 すべてのデバイスの設定変更をプレビューして展開します。

Security Cloud Control のネットワークオブジェクトとグループの削除

クラウド提供型 Firewall Management Center がテナントにデプロイされている場合：

オブジェクト ページからネットワークオブジェクトまたはグループを削除すると、クラウド提供型 Firewall Management Center の **オブジェクト** ページから重複するネットワークオブジェクトまたはグループが削除されます。その逆も同様です。

ネットワークオブジェクトの検出と管理オンプレミス Firewall Management Center

Security Cloud Control を使用して管理する オンプレミス Firewall Management Center があり、そのオブジェクトを共有および管理する場合は、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** の順に選択して、[Services] ページを表示します。

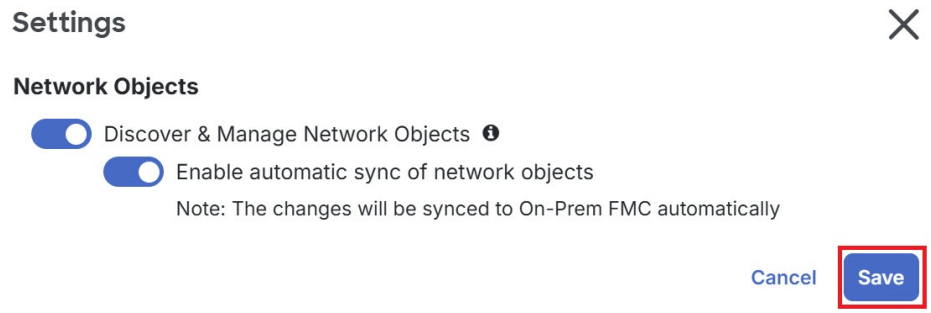
ステップ 2 すでに オンプレミス Firewall Management Center が Security Cloud Control にオンボード済みの場合は、それを選択します。

新たに オンプレミス Firewall Management Center をオンボードする場合は、「オンプレミス Firewall Management Center のオンボード」を参照してください。

ステップ 3 右側の [Actions] ペインから [Settings] を選択します。複数の オンプレミス Firewall Management Center を選択しても、**[Actions]** ペインは表示されません。

（注）
[Settings] を使用するには、管理者またはネットワーク管理者である必要があります。

ステップ 4 [ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルボタンを有効にします。変更を オンプレミス Firewall Management Center と自動的に同期し、確認のためのステージングをしない場合は、**[Enable automatic sync of network objects]** トグルをオンにします。次に [Save] をクリックします。



（注）

- 選択した オンプレミス Firewall Management Center に 1 つ以上の子ドメインがある場合、または変更管理ワークフローが有効になっている場合は、[Discover & Manage Network Objects] トグルをオンにできません。
- [Discover & Manage Network Objects] がオフの場合は、[Enable automatic sync of network objects] トグルをオンにできません。

Security Cloud Control に新しい オンプレミス Firewall Management Center をオンボードするたびに、このトグルボタンを手動で有効にする必要があります。このオプションを有効にすると、Security Cloud Control はオンプレミス Firewall Management Center からオブジェクトを検出します。これらのオブジェクトを共有して管理し、Security Cloud Control によって管理される他のプラットフォーム間で一貫したオブジェクト定義を設定するために使用できます。

Security Cloud Control では、オンプレミス Firewall Management Center から検出されたオブジェクトにオーバーライドを追加し、変更をプッシュすると、以前はオーバーライドが許可されなかった場合でも、これらのオブジェクトをオーバーライドできるようになりました。**[View Network Object]** ウィンドウの **[Allow Overrides]** チェックボックスは、Security Cloud Control からオーバーライドを追加すると自動的に選択されます。

（注）
Security Cloud Control 内の既存のオブジェクトを オンプレミス Firewall Management Center に割り当てる場合は、オンプレミス Firewall Management Center を選択し、[アクション（Actions）] ペインで [オブジェクトの割り当て（Assign Objects）] をクリックします。

関連情報

- ネットワーク オブジェクト
- オンプレミス Firewall Management Center の設定のプレビューと展開
- オンプレミス Firewall Management Center の競合検出の有効化

サービス オブジェクト

プロトコルオブジェクト

プロトコルオブジェクトは、使用頻度の低いプロトコルやレガシープロトコルを含むサービスオブジェクトの一種です。プロトコルオブジェクトは、名前とプロトコル番号によって識別されます。Security Cloud Control は、ASA および Firepower（FDM による管理 デバイス）設定でこれらのオブジェクトを認識し、これらに独自のフィルタ「プロトコル」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

ICMP オブジェクト

Internet Control Message Protocol（ICMP）オブジェクトは、ICMP および IPv6-ICMP メッセージ専用のサービスオブジェクトです。Security Cloud Control は、ASA および Firepower がオンボー

ドされたときにデバイスの設定でこれらのオブジェクトを認識し、これらに Security Cloud Control が独自のフィルタ「ICMP」を適用します。そのため、これらのオブジェクトを簡単に見つけることができます。

Security Cloud Control を使用して、ASA 設定から ICMP オブジェクトの名前を変更したり、ICMP オブジェクトを削除したりできます。Security Cloud Control を使用して、Firepower 設定の ICMP および ICMPv6 オブジェクトを作成、更新、および削除できます。

（注） ICMPv6 プロトコルの場合、AWS は特定の引数の選択をサポートしていません。すべての ICMPv6 メッセージを許可するルールのみがサポートされます。

関連情報：

- オブジェクトの削除 （33 ページ）

ネットワーク アドレス変換

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、企業のプライベートネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

ネットワーク アドレス変換（NAT）の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるためです。

NAT の他の機能には、次のおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティングソリューション：NAT を使用する際に、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリックアドレスに影響を与えずに、内部 IP アドレス方式を変更できます。たとえば、インターネットにアクセス可能なサーバーの場合、インター

ネット用に固定 IP アドレスを維持できますが、内部向けにサーバーのアドレスを変更することができます。

- IPv4 と IPv6（ルーテッドモードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

Security Cloud Control を使用して、さまざまな使用例の NAT ルールを作成できます。NAT ルールウィザードまたは次のトピックを使用して、さまざまな NAT ルールを作成します。

NAT ルールの処理命令

ネットワークオブジェクトの NAT ルールおよび Twice NAT ルールは、3 つセクションに分割された 1 つのテーブルに格納されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 *5 : NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	Twice NAT（ASA） 手動 NAT（FTD）	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 2	ネットワークオブジェクト NAT（ASA） 自動 NAT（FTD）	セクション1で一致が見つからない場合、セクション2のルールが次の順序で適用されます。 **1.** スタティックルール **2.** ダイナミックルール **各ルールタイプでは、次の順序ガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じIPアドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、オブジェクト「Arlington」はオブジェクト「Detroit」の前に評価されます。
セクション 3	Twice NAT（ASA） 手動 NAT（FTD）	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）
- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト Detroit）

- 172.16.1.0/24（ダイナミック）（オブジェクト Arlington）

この結果、使用される順序は次のとおりです。

- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト Arlington）
- 172.16.1.0/24（ダイナミック）（オブジェクト Detroit）
- 192.168.1.0/24（ダイナミック）

ネットワークアドレス変換ウィザード

ネットワークアドレス変換（NAT）ウィザードは、次のタイプのアクセスに使用するNATルールをデバイスで作成する際に役立ちます。

- **内部ユーザーのインターネットアクセスを有効にする**。この NAT ルールを使用して、内部ネットワーク上のユーザーがインターネットにアクセスできるようにすることができます。
- **内部サーバーをインターネットに公開する**。この NAT ルールを使用して、ネットワーク外のユーザーが内部 Web サーバーまたは電子メールサーバーにアクセスできるようにすることができます。

「内部ユーザーのインターネットアクセスを有効にする」ための前提条件

NAT ルールを作成する前に、次の情報を収集します。

- ユーザーに最も近いインターフェイス。通常これは「内部」インターフェイスと呼ばれます。
- インターネット接続に最も近いインターフェイス。通常これは「外部」インターフェイスと呼ばれます。
- 特定のユーザーのみにインターネットへのアクセスを許可する場合は、それらのユーザーのサブネットアドレスが必要です。

「内部サーバーをインターネットに公開する」ための前提条件

NAT ルールを作成する前に、次の情報を収集します。

- ユーザーに最も近いインターフェイス。通常これは「内部」インターフェイスと呼ばれます。

- インターネット接続に最も近いインターフェイス。通常これは「外部」インターフェイスと呼ばれます。
- インターネット側の IP アドレスに変換する、ネットワーク内のサーバーの IP アドレス。
- サーバーが使用するパブリック IP アドレス。

次の作業

NAT ウィザードを使用した NAT ルールの作成 （62 ページ） を参照してください。

NAT ウィザードを使用した NAT ルールの作成

始める前に

NAT ウィザードを使用して NAT ルールを作成するために必要な前提条件については、ネットワークアドレス変換ウィザード （61 ページ）を参照してください。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 [Filter]と[Search]フィールドを使用して、NAT ルールを作成するデバイスを見つけます。

ステップ 5 詳細パネルの [管理（Management）] 領域で、[NAT] NAT をクリックします。

ステップ 6 + > [NAT ウィザード（NAT Wizard）] をクリックします。

ステップ 7 NAT ウィザードの質問に回答し、画面の指示に従います。

- NAT ウィザードはネットワーク オブジェクト （35 ページ）を使用してルールを作成します。ドロップダウンメニューから既存のオブジェクトを選択するか、作成ボタン + Create... で新しいオブジェクトを作成します。
- NAT ルールを保存する前に、すべての IP アドレスをネットワークオブジェクトとして定義する必要があります。

ステップ 8 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

NAT の一般的な使用例

Twice NAT と手動 NAT

「自動 NAT」とも呼ばれる「ネットワークオブジェクト NAT」を使用して達成できるいくつかの一般的なタスクを次に示します。

- 内部ネットワーク上のサーバーがパブリック IP アドレスを使用してインターネットに到達できるようにする （63 ページ）
- 内部ネットワーク上のユーザーが外部インターフェイスのパブリック IP アドレスを使用してインターネットにアクセスできるようにする （65 ページ）
- 内部ネットワーク上のサーバーをパブリック IP アドレスの特定のポートで使用できるようにする （66 ページ）
- プライベート IP アドレス範囲のパブリック IP アドレス範囲への変換 （70 ページ）

ネットワークオブジェクト NAT と自動 NAT

「手動 NAT」とも呼ばれる「Twice NAT」を使用して達成できる一般的なタスクを次に示します。

- 外部インターフェイスを通過する際に IP アドレスの範囲が変換されるのを防ぐ （71 ページ）

内部ネットワーク上のサーバーがパブリックIPアドレスを使用してインターネットに到達できるようにする

使用例

インターネットからアクセスする必要があるプライベートIPアドレスを持つサーバーがあり、1 つのパブリック IP アドレスからプライベート IP アドレスへの NAT に十分なパブリック IP アドレスがある場合は、この NAT 戦略を使用します。パブリック IP アドレスの数に限りがある場合は、「パブリック IP アドレスの特定のポートでユーザーが内部ネットワーク上のサーバーを使用できるようにする」を参照してください（このソリューションの方が適している可能性があります）。

方法

サーバーは静的なプライベートIPアドレスを持ち、そのサーバーにネットワークの外部のユーザーがアクセスできる必要があります。静的プライベート IP アドレスを静的パブリック IP アドレスに変換するネットワークオブジェクトNATルールを作成します。その後、そのパブリック IP アドレスからのトラフィックがプライベート IP アドレスに到達できるようにするアクセスポリシーを作成します。最後に、これらの変更をデバイスに展開します。

始める前に

まず始めに、2 つのネットワークオブジェクトを作成します。一方のオブジェクトを「*servername*_inside」と名前を付け、もう一方のオブジェクトに「*servername*_outside」という名前を付けます。*servername*_inside ネットワークオブジェクトには、サーバーのプライベート IP アドレスが含まれている必要があります。*servername*_outside ネットワークオブジェクトには、サーバーのパブリック IP アドレスが含まれている必要があります。

手順については、「ネットワークオブジェクトの作成」を参照してください。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  > [ネットワークオブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

1. [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、**servername_inside** オブジェクトを選択します。
2. [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、**servername_outside** オブジェクトを選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 FDM 管理対象デバイスの場合、セクション 5 の [名前（Name）] で、NAT ルールに名前を付けます。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 ASA の場合はネットワークポリシー規則を展開し、FDM による管理 デバイスの場合はアクセス コントロール ポリシー規則を展開して、*servername*_inside から *servername*_outside へのトラフィックフローを可能にします。

ステップ 14 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

内部ネットワーク上のユーザーが外部インターフェイスのパブリック IP アドレスを使用してインターネットにアクセスできるようにする

使用例

外部インターフェイスのパブリックアドレスを共有することにより、プライベートネットワーク内のユーザーとコンピューターがインターネットに接続できるようにします。

方法

プライベートネットワーク上のすべてのユーザーがデバイスの外部インターフェイスのパブリック IP アドレスを共有できるようにするポートアドレス変換（PAT）ルールを作成します。

プライベートアドレスがパブリックアドレスとポート番号にマッピングされると、デバイスはそのマッピングを記録します。そのパブリック IP アドレスとポート宛の着信トラフィックを受信すると、デバイスはトラフィックを要求したプライベート IP アドレスにトラフィックを送り返します。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  [ネットワークオブジェクトNAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で、[ダイナミック（Dynamic）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [任意（any）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

1. [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、ネットワーク構成に応じて [any-ipv4] オブジェクトまたは [any-ipv6] オブジェクトを選択します。
2. [変換済みアドレス（Translated Address）] メニューを展開し、利用可能なリストから [インターフェイス（interface）] を選択します。インターフェイスにより、外部インターフェイスのパブリックアドレスを使用することが示唆されています。

ステップ 10 FDM 管理対象デバイスの場合、セクション 5 の [名前（Name）] に NAT ルールの名前を入力します。

ステップ 11 [保存（Save）] をクリックします。

ステップ 12 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

ASA の保存済み構成ファイルのエントリ

この手順を実行することで、ASA の保存済み構成ファイル内に次のエントリが作成および表示されます。

（注） これは FDM による管理 デバイスには適用されません。

この手順によって作成されるオブジェクト：

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

この手順によって作成される *NAT* ルール：

```
object network any_network
nat (any,outside) dynamic interface
```

内部ネットワーク上のサーバーをパブリックIPアドレスの特定のポートで使用できるようにする

使用例

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

前提条件

まず始めに、FTP、HTTP、および SMTP サーバーのネットワークオブジェクトを 1 つずつ、合計 3 つの個別のオブジェクトを作成します。この手順のために、これらのオブジェクトを **ftp-server-object**、**http-server-object**、および **smtp-server-object** と呼びます。

手順については、「」「」を参照してください。

FTP サーバーへの NAT 着信 FTP トラフィック

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 > [ネットワークオブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、**ftp**-server-object を選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- [tcp]、[ftp]、[ftp] を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 FDM 管理対象デバイスの場合、セクション 5 の [名前（Name）] で、NAT ルールに名前を付けます。

ステップ 12 [保存（Save）] をクリックします。NAT テーブルの セクション 2 に新しいルールが作成されます。

ステップ 13 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

HTTP サーバーへの NAT 着信 HTTP トラフィック

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

始める前に

まず始めに、HTTP サーバーのネットワークオブジェクトを作成します。この手順のために、オブジェクトを **http-object** と呼びます。

手順については、「」「」を参照してください。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 > [ネットワークオブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [オリジナルアドレス（Original Address）] メニューを展開し、[選択]（Choose）] をクリックして、**http** オブジェクトを選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- **tcp**、**http**、http を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 FDM 管理対象デバイスの場合、セクション 5 の [名前（Name）] で、NAT ルールに名前を付けます。

ステップ 12 [保存（Save）] をクリックします。NAT テーブルの セクション 2 に新しいルールが作成されます。

ステップ 13 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

SMTP サーバーへの NAT 着信 SMTP トラフィック

パブリック IP アドレスが 1 つしかない場合、または数が非常に限られている場合は、静的 IP アドレスとポートにバインドされた受信トラフィックを内部アドレスに変換するネットワークオブジェクト NAT ルールを作成できます。特定のケースの手順を提供していますが、これらはサポートされている他のアプリケーションのモデルとして使用できます。

始める前に

まず始めに、smtp サーバーのネットワークオブジェクトを作成します。この手順の説明では、オブジェクトを **smtp-object** と呼びます。

手順については、「」「」を参照してください。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  > [ネットワークオブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次のアクションを実行します。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、smtp-server-object を選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択]（Choose）] をクリックして、[インターフェイス（Inerface）] を選択します。
- [ポート変換の使用（Use Port Translation）] にチェックを付けます。
- tcp、smtp、smtp を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 FDM 管理対象デバイスの場合、セクション 5 の [名前（Name）] で、NAT ルールに名前を付けます。

ステップ 12 [保存（Save）] をクリックします。NAT テーブルの セクション 2 に新しいルールが作成されます。

ステップ 13 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

プライベート IP アドレス範囲のパブリック IP アドレス範囲への変換

使用例

特定のデバイスタイプまたはユーザータイプのグループがあり、IPアドレスを特定の範囲に変換して、受信側デバイス（トランザクションの反対側のデバイス）がトラフィックを許可する必要がある場合は、このアプローチを使用します。

内部アドレスのプールを外部アドレスのプールに変換

始める前に

変換するプライベート IP アドレスプールのネットワークオブジェクトを作成し、それらのプライベート IP アドレスの変換先となるパブリックアドレスプールのネットワークオブジェクトも作成します。

（注） ASA の場合、「変換されたアドレス」のプールを定義するネットワークグループは、サブネットを定義するネットワークオブジェクトにすることはできません。

これらのアドレスプールを作成する場合は、とを参照してください。

以下の手順のために、プライベートアドレスプールを**inside_pool**、パブリックアドレスプールを**outside_pool** と名付けました。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6 > [ネットワーク オブジェクト NAT（Network Object NAT）] をクリックします。

ステップ 7 セクション 1 の [タイプ（Type）] で [ダイナミック（Dynamic）] を選択し、[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスを [内部（inside）] に設定し、接続先インターフェイスを [外部（outside）] に設定します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、以下のタスクを実行します。

- [元アドレス（Original Address）] で、[選択（Choose）] をクリックし、上記の前提条件セクションで作成した **inside_pool** ネットワークオブジェクト (またはネットワークグループ) を選択します。

- [変換されたアドレス（Translated Address）] で、[選択（Choose）] をクリックし、上記の前提条件セクションで作成した **outside_pool** ネットワークオブジェクト (またはネットワークグループ) を選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 FDM 管理対象デバイスの場合、セクション 5 の [名前（Name）] で、NAT ルールに名前を付けます。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

外部インターフェイスを通過する際にIPアドレスの範囲が変換されるのを防ぐ

使用例

この Twice NAT ユースケースを使用して、サイト間 VPN を有効にします。

方法

IP アドレスのプールをそれ自体に変換して、ネットワークのある場所の IP アドレスが変更されずに別の場所に届くようにします。

Twice NATルールの作成

始める前に

それ自体に変換する IP アドレスのプールを定義するネットワークオブジェクトまたはネットワークグループを作成します。ASA の場合、アドレスの範囲は、IP アドレス範囲を使用するネットワークオブジェクト、サブネットを定義するネットワークオブジェクト、または範囲内のすべてのアドレスを含むネットワーク グループ オブジェクトによって定義できます。

ネットワークオブジェクトやネットワークグループを作成する場合は、『』と『』を参照してください。

次の手順では、ネットワークオブジェクトまたはネットワークグループを Site-to-Site-PC-Pool と呼びます。

手順

ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 NAT ルールを作成するデバイスを選択します。

ステップ 5 右側の [管理（Management）] ペインで [NAT] をクリックします。

ステップ 6  > [Twice NAT] をクリックします。.

ステップ 7 セクション 1 の [タイプ（Type）] で、[静的（Static）] を選択します。[続行（Continue）] をクリックします。

ステップ 8 セクション 2 の [インターフェイス（Interfaces）] で、送信元インターフェイスには [内部（inside）] を選択し、接続先インターフェイスには [外部（outside）] を選択します。[続行（Continue）] をクリックします。

ステップ 9 セクション 3 の [パケット（Packets）] で、次の変更を行います。

- [元のアドレス（Original Address）] メニューを展開し、[選択（Choose）] をクリックして、前提条件セクションで作成した Site-to-Site-PC-Pool オブジェクトを選択します。
- [変換済みアドレス（Translated Address）] メニューを展開し、[選択（Choose）] をクリックして、前提条件セクションで作成した Site-to-Site-PC-Pool オブジェクトを選択します。

ステップ 10 セクション 4 の [詳細（Advanced）] はスキップしてください。

ステップ 11 FDM 管理対象デバイスの場合、セクション 5 の [名前（Name）] で、NAT ルールに名前を付けます。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 ASA の場合、クリプトマップを作成します。クリプトマップの作成方法の詳細については、『CLI ブック 3：Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド』の、「LAN-to-LAN IPsec VPN」の章を確認してください。

ステップ 14 行った変更を今すぐレビューして展開するか、待機してから複数の変更を一度に展開します。

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