ASA デバイスを設定する

この章は、次のセクションで構成されています。

ASA の接続ログイン情報の更新

ASA の導入準備プロセスで、CDO がデバイスに接続するために使用する必要があるユーザー名とパスワードを入力しました。これらのログイン情報がデバイスで変更された場合は、**ログイン情報の更新**のデバイスアクションを使用して、CDO でもログイン情報を更新します。この機能により、デバイスを再度導入準備することなく、CDO でログイン情報を更新できます。切り替えるユーザー名とパスワードの組み合わせは、ユーザーの ASA または認証、許可、およびアカウンティング（AAA）サーバーにすでに存在している必要があります。このプロセスは、Cisco Defense Orchestrator データベースにのみ影響します。ログイン情報の更新機能を使用しても、ASA の構成は変更されません。

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックしてから、[ASA] をクリックします。

ステップ 3 接続ログイン情報を更新する ASA を選択します。1 つ以上の ASA のログイン情報を一度に更新できます。

ステップ 4 [デバイスアクション] ペインで、[ログイン情報の更新] をクリックします。

ステップ 5 ASA を CDO に接続するために使用する Cloud Connector または Secure Device Connector（SDC）を選択します。

ステップ 6 ASA への接続に使用する新しいユーザー名とパスワードを入力します。

ステップ 7 ログイン情報が変更されると、CDO はデバイスを同期します。

（注） CDO がデバイスの同期に失敗した場合、CDO の接続ステータスに [無効なログイン情報] と表示されることがあります。その場合は、無効なユーザー名とパスワードの組み合わせを使用した可能性があります。使用するログイン情報が ASA または AAA サーバーに保存されていることを確認して、再試行してください。

ある SDC から別の SDC への ASA の移動

CDO では、テナントごとに複数の SDC の使用をサポートしています。次の手順を使用して、管理対象 ASA を、ある SDC から別の SDC に移動できます。

ステップ 1 CDO メニューバーから、[デバイスとサービス] をクリックします。

ステップ 2 別の SDC に移動する ASA を選択します。

ステップ 3 [デバイスアクション] ウィンドウで、[ログイン情報の更新（Update Credentials）] をクリックします。

ステップ 4 [セキュアデバイスコネクタ（Secure Device Connector）] ボタンをクリックし、デバイスの移動先の SDC を選択します。

ステップ 5 ASA の導入準備に使用した管理者のユーザー名とパスワードを入力し、[更新（Update）] をクリックします。これらの変更をデバイスに展開する必要はありません。

オブジェクト

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。

デバイスを導入準備すると、CDO 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] ページにリストします。[オブジェクト] 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。

CDO では、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] 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。

[オブジェクト]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、CDO によって管理されているオブジェクトを表示できます。

CDO 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。CDO 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オブジェクトフィルタします。
- 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。
- 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 CDO に導入準備された後、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。

導入準備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、CDO 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、CDO 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 *1*:適応型セキュリティアプライアンス（*ASA*）のオブジェクトタイプ

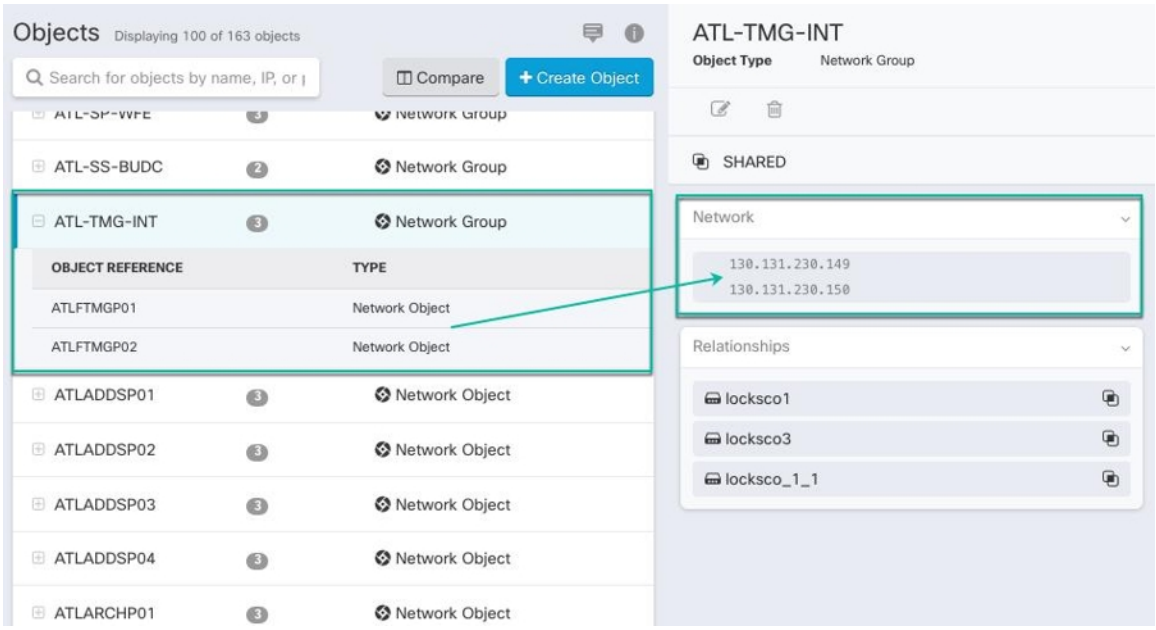
オブジェクト	説明
IP アドレスプールの作成	アドレスプールオブジェクトは、個々の IPv4 または IPv6 アドレス、または IP アドレス範囲と照合するように設定できます。
RA VPN AnyConnect クライアントプロファイルのアップロード	AnyConnect クライアント プロファイル オブジェクトは、ファイルオブジェクトで、通常はリモートアクセス VPN ポリシーの構成で使用するファイルを表します。このオブジェクトには、AnyConnect クライアントプロファイルと AnyConnect クライアント イメージ ファイルを含めることができます。
ネットワーク オブジェクト	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 オブジェクト	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。
ASA 時間範囲オブジェクト	時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能またはアセットに時間ベースでアクセスするためにネットワークポリシーで使用されます。
トラストポイントのオブジェクト	トラストポイントを使用すると、ASA でデジタル証明書を管理および追跡できます。

共有オブジェクト

Cisco Defense Orchestrator（CDO）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]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、CDO 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。CDO 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、特定のデバイス上の共有ネットワークオブジェクトの値をオーバーライドできます。CDO は、オーバーライドを構成するときに指定したデバイスに対応する値を使用します。これらのオブジェクトは、名前は同じで値が異なる複数のデバイス上にありますが、CDO は、これらの値がオーバーライドとして追加されただけでは、それらを**不整合オブジェクト**として識別しません。

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、各オフィスにプリンタサーバーがあり、プリンタサーバーオブジェクト `print-server` を作成しているシナリオを考えてみましょう。ACL には、プリンタサーバーのインターネットへのアクセスを拒否するルールを設定しています。プリンタ サーバー オブジェクトには、オフィスごとに変更できるデフォルト値があります。これを行うには、オブジェクトのオーバーライドを使用し、すべての場所でルールと「printer-server」オブジェクトの一貫性を維持します（値は異なる場合があります）。

（注） 一貫性のないオブジェクトがある場合は、オーバーライドを使用してそれらを1つの共有オブジェクトに結合できます。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。

オブジェクトの比較

ステップ1 [オブジェクト] ページを開きます。

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 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] 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] ボックスと [関係] 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] 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] をクリックして、デバイスの構成を表示できます。CDO 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

[インベントリ] ページと [オブジェクト] 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およびオブジェクトを見つけることができます。

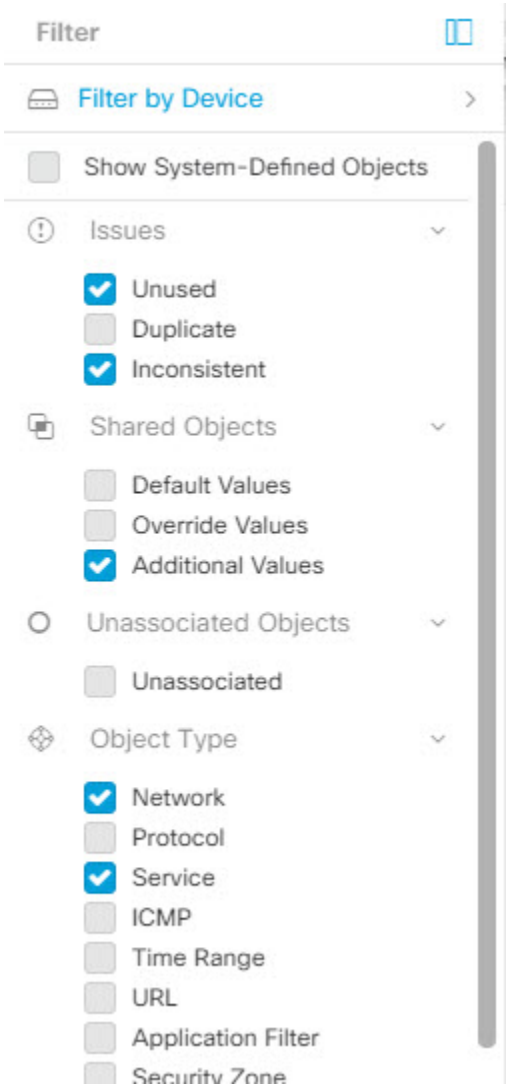
フィルタ処理するには、[デバイスとサービス（Devices and Services）] タブ、[ポリシー（Policies）] タブ、および [オブジェクト] タブの左側のペインで をクリックします。

インベントリフィルタでは、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。

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（使用されている、または、不整合）があるオブジェクト、かつ、追加の値を持つ共有オブジェクト、かつ、特定のタイプ（ネットワーク、または、サービス）のオブジェクト」であるような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] タブの左側のペインで をクリックします。

- [すべてのオブジェクト]：このフィルタは、CDO で導入準備したすべてのデバイスから使用可能なすべてのオブジェクトを提供します。このフィルタは、すべてのオブジェクトを参照するために、または検索の開始点として、さらにサブフィルタを適用するために役立ちます。

- [共有オブジェクト]：このクイックフィルタは、複数のデバイスで共有されていることがCDO によって検出されたすべてのオブジェクトを表示します。
- [デバイスごとのオブジェクト]：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。

[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] をクリックしてデバイスを指定します）。AND

* **一貫性のない**オブジェクト AND

* **ネットワーク**オブジェクト OR **サービス**オブジェクト AND

* 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を表示] 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。

システムオブジェクトを表示フィルタ

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。

[システムオブジェクトを表示] はデフォルトで [オフ] です。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 [システムオブジェクトを表示] 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] 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。

ステップ 1 ナビゲーションバーで [オブジェクト] をクリックして、[オブジェクト] ページを表示します。

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]** 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] 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] をオフにします。

ステップ 5 [問題] 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] 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] 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] 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。CDO が識別するオブジェクトを選択し、[関係]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 CDO 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。

ステップ 1 [オブジェクト] ページを開きます。

ステップ 2 オブジェクトフィルタ。

ステップ 3 [オブジェクト] 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

1 つのオブジェクトを削除するには、次の手順を実行します。

ステップ 1 [オブジェクト] タブをクリックして、[オブジェクト] ページを開きます。

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] 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] ペインで、[削除] 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 行った変更をすべてのデバイスの構成変更のプレビューと展開か、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

デバイスを導入準備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。

ステップ 1 [問題] 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] ペインで、[削除] 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すべてのデバイスの構成変更のプレビューと展開か、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**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集合体です。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。CDO 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。

表 *2:* ネットワークオブジェクトで許可される値

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	完全修飾ドメイン名	CIDR 表記法によるサブネット
ASA	IPv4	対応	対応	対応	対応

表 *3:* ネットワークグループで許可される内容

デバイス タイプ（Device Type）	IP 値	[ネットワーク オブジェクト（Network Object）]	ネットワーク グループ
ASA	対応	対応	対応

ネットワークオブジェクトの表示

CDO を使用して作成するネットワークオブジェクトと、導入準備したデバイスの設定から CDO が認識するネットワークオブジェクトは、[オブジェクト] 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] 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] 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。CDO 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。

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 表記によるサブネット
ASA	IPv4	対応	対応	対応	対応

ASA ネットワークオブジェクトの作成

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] 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] 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] 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。

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（Network Group）] 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。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] 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 CDO 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 CDO 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、[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 12 すべてのデバイスの構成変更のプレビューと展開 （178 ページ）。

ASA ネットワークオブジェクトの編集

ステップ 1 ナビゲーションバーで、[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、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] 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。CDO 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

ステップ 1 ナビゲーションバーで、[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、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] 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CDO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. CDO 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] 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として追加（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。CDO は、変更の影響を受けるポリシーを表示します。

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構成変更のプレビューと展開 （178 ページ）。

共有ネットワークグループへの追加の値の追加

関連付けられた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内の値は、「デフォルト値」と呼ばれます。CDO 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、それらの値をその共有ネットワークグループに関連付けられたいくつかのデバイスに割り当てることができます。CDO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、ブランチオフィス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。

ステップ 1 ナビゲーションバーで、[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、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] ペインにある編集アイコン をクリックします。

- [デバイス] 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（Default Values）] 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 CDO 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 CDO 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] 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。CDO 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構成変更のプレビューと展開 （178 ページ）。

共有ネットワークグループの追加の値の編集

ステップ 1 ナビゲーションバーで、[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、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。CDO 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構成変更のプレビューと展開 （178 ページ）。

トラストポイントのオブジェクト

CDO を使用して、デジタル証明書をトラストポイント オブジェクトとして追加し、1 つまたは複数の管理対象 ASA デバイスにインストールできます。単一のトラストポイント オブジェクトは、アイデンティティペア（ID 証明書と発行者の CA 証明書）、ID 証明書のみ、または CA 証明書のみを保持するコンテナです。

ASAデバイスには多くのトラストポイントを設定できます。サポートされている証明書形式はPKCS12、PEM、DERです。

PKCS12 を使用したID 証明書オブジェクトを追加する

この手順では、証明書ファイルをアップロードするか、既存の証明書テキストをテキストボックスに貼り付けることで、内部証明書アイデンティティまたは内部ID 証明書を作成します。必要な数のID 証明書を生成できます。

PKCS12 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。PKCS12 は、CA サーバー証明書、中間証明書、秘密キーを 1 つの暗号化されたファイルで保持する単一のファイルです。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。復号のための [パスフレーズ（Passphrase）] 値を入力します。

ステップ 1 ナビゲーションバーで、[オブジェクト] > [ASA] > [トラストポイント] を選択します。

ステップ 2 証明書の [オブジェクト名] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [証明書タイプ] ステップで、[ID 証明書] を選択します。

ステップ 4 [インポートタイプ] ステップで、[アップロード] を選択して証明書ファイルをアップロードします。

[登録] ステップは [端末] に設定されています。

ステップ 5 [証明書の内容] ステップで、PKCS12 形式の詳細を入力します。

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。復号のための [パスフレーズ（Passphrase）] 値を入力します。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 [詳細オプション] ステップでは、以下を設定できます。

[失効] タブでは、以下を設定できます。

- [証明書失効リスト（CRL）の有効化]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布 URL を取得するために [証明書のCRL分散ポイントを使用する] チェックボックスがオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは60分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

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

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

  [ナンス拡張を無効化]：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張

を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバーから、事前に生成した応答を送信する場合は、[ナンス拡張を無効化] チェックボックスをオフにしてください。

[評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェック ボックスをオンにします。

  失効チェックの詳細については、『 Cisco ASA Series General Operations ASDM Configuration、X.Y』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA証明書を使用]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。
  - [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。
- [ID 証明書の使用]：登録済み ID 証明書の使用方法を指定します。
  - [SSL & IPSec]：SSL & IPSec 接続の認証に使用します。
  - [コード署名者] ：コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。
- **その他のオプション**：
  - [基本制約拡張でCAフラグを有効化する]：この証明書で他の証明書に署名できるようにする場合はこのオプションをオンにします。基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。証明書におけるこれらの項目のプレゼンス
  - [このCAが発行した証明書を受け入れる]：指定した CA の証明書を ASA で受け入れるようにするにはこのオプションを選択します。
  - [IPsecキーの使用状況を無視]：IPsec リモートクライアント証明書のキーの使用状況および拡張キーの用途拡張の値を検証しない場合は、このオプションを選択します。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、このオプションはイネーブルになっていません。

ステップ 8 [追加（Add）] をクリックします。

自己署名済みID 証明書オブジェクトを作成する

この手順では、ウィザードに適切な証明書フィールド値を入力することにより、自己署名証明書を生成する手順を説明します。自己署名証明書は必要な数だけ生成できます。

自己署名済みID 証明書オブジェクトを作成するには、次の手順を実行します。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] > [ASA] > [トラストポイント（Trustpoints）] を選択します。

ステップ 2 証明書の [オブジェクト名（Object Name）] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [証明書タイプ] ステップで、[ID 証明書（Identity Certificate）] を選択します。

ステップ 4 [インポートタイプ] ステップで、[新規（New）] を選択して証明書ファイルをアップロードし、[続行] をクリックします。

ステップ 5 [登録] ステップで、[自己署名済み（Self-Signed）] を選択し、[続行] をクリックします。

証明書の内容のステップが表示されます。「証明書コンテンツに基づく自己署名済みCSR 証明書の生成」を読んで、生成されている自己署名付き証明書の CN および SANS コンテンツを理解してください。

ステップ 6 [証明書の内容（Certificate Contents）] の手順で、次の設定を行います。

- [国（C）（Country (C)）]：ドロップダウトリストから国コードを選択します。
- [都道府県（ST）（State or Province (ST)）]：証明書に含める都道府県または州。
- [地域または都市（L）（Locality or City (L)）]：都市の名前など、証明書に含める地域。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [組織単位（部門）（OU）（Organizational Unit (Department) ）]：証明書に含める組織単位の名前（部門名など）。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。これは、デバイスの名前、Web サイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモート アクセス VPN で使用する内部証明書に CN を含める必要があります。
- [電子メールアドレス（EA）（Email Address (EA)）]：ID 証明書に関連付けられている電子メールアドレス。
- [IPアドレス（IP Address）]：4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレス。
- [デバイスのFQDN（Device's FQDN）]：DNS ツリー階層内のノードの位置を示す完全修飾ドメイン名。
- [デバイスのシリアル番号を含める（Include Device's Serial Number）]：ASA のシリアル番号を証明書パラメータに追加するには、チェックボックスをオンにします。

a) [キー（Key）] タブをクリックします。

- **RSA** または **ECDSA** キーのタイプを選択します。

- [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。推奨されるキーのサイズは、RSA では 1024、ECDSA では 348 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。
- [続行（Continue）] をクリックします。

ステップ 7 [詳細オプション] ステップでは、以下の設定を行うことができます。

[失効] タブでは、以下の設定を行うことができます。

- [証明書失効リスト（CRL）の有効化）]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布 URL を取得するために、[証明書からのCRL配布ポイントの使用] がオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

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

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

  [ナンス拡張子を無効化] ：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。使用している OCSP サーバーから、この一致するナンス拡張子を含まない事前に生成した応答を送信する場合は、[ナンス拡張子を無効化] チェックボックスをオフにしてください。

  [評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェックボックスをオンにします。

  失効チェックの詳細については、『Cisco ASA Series General Operations ASDM Configuration、XY』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA証明書を使用（Use CA Certificate for the Validation of）]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。

- [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。

- [ID証明書の使用]：登録済み ID 証明書の使用方法を指定します。
  - [SSL & IPSec]：SSL & IPSec 接続の認証に使用します。
  - [コード署名者]：コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

- **その他のオプション**：
  - [基本制約拡張でCAフラグを有効化する]：この証明書で他の証明書に署名できるようにする場合はこのオプションをオンにします。基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。証明書におけるこれらの項目の存在
  - [このCAが発行した証明書を受け入れる（Accept certificates issued by this CA）]：指定した CA の証明書を ASA で受け入れるようにするにはこのチェックボックスをオンにします。
  - [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）]：IPsec リモートクライアント証明書のキーの使用状況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、このオプションを選択します。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、このオプションはイネーブルになっていません。

ステップ 8 [追加（Add）] をクリックします。

証明書署名要求（CSR）用 ID 証明書オブジェクトを追加する

証明書署名要求（CSR）を生成したり、指定されたCAからID証明書を取得したりするためには、認証局（CA）サーバー情報と登録パラメータが必要です。要求を生成するには、Rivest-Shamir-Adleman（RSA）または楕円曲線デジタル署名アルゴリズム（楕円曲線DSA）のいずれかのキータイプを選択する必要があります。

識別情報を提供し、オプションで CA から取得した CA 証明書をアップロードして、トラストポイント オブジェクトを作成します。

ステップ 1 ナビゲーションバーで、[オブジェクト] > [ASA] > [トラストポイント] を選択します。

ステップ 2 証明書の [オブジェクト名] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [ID証明書] ステップで、[ID証明書] を選択します。

ステップ 4 [インポートタイプ] ステップで、[新規] を選択して証明書ファイルをアップロードし、[続行] をクリックします。

ステップ 5 [登録] ステップで、[手動] を選択します。

ステップ 6 （オプション）CA から取得した CA 証明書を貼り付けるか、アップロードできます。このフィールドは空のままにすることもできます。

ステップ 7 [続行（Continue）] をクリックします。

証明書の内容のステップが表示されます。「証明書コンテンツに基づく自己署名済み CSR 証明書の生成」を読んで、生成されている署名付き証明書の CN および SANS コンテンツを理解してください。

ステップ 8 [証明書の内容] の手順で、次の設定を行います。

- [国（C）]：ドロップダウトリストから国コードを選択します。
- [都道府県（ST）]：証明書に含める都道府県または州。
- [地域または都市（L）]：都市の名前など、証明書に含める地域。
- [組織（O）（Organization (O)）]：証明書に含める組織または会社の名前。
- [組織単位（部門）（OU）]：証明書に含める組織単位の名前（部門名など）。
- [共通名（CN）（Common Name (CN)）]：証明書に含める X.500 共通名。これは、デバイスの名前、Web サイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモート アクセス VPN で使用する内部証明書に CN を含める必要があります。
- [電子メールアドレス（EA）]：ID 証明書に関連付けられている電子メールアドレス。
- [IPアドレス]：4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレス。
- [サブジェクトの別名 （SAN）]：このフィールドは、「unstructuredName」として証明書のサブジェクト DN の一部にもなります。証明書が複数のドメインまたは IP アドレスに使用される場合は、このフィールドを使用することをお勧めします。
  - [デバイスのホスト名を使用]：デバイスのホスト名が使用されます。
  - [カスタム：デバイスのFQDN]：DNS ツリー階層内のノードの位置を示す明確なドメイン名。

    （注） CN と**カスタム FQDN** で指定する値は同じにすることを推奨します。

- [デバイスのシリアル番号を含める]：ASA のシリアル番号を証明書に含めるには、チェックボックスをオンにします。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。

a) [キー] タブをクリックします。

- **RSA** または **ECDSA** キーのタイプを選択します。
- [キーサイズ]：キーペアが存在しない場合は、必要なキーサイズ（係数）をビット単位で定義します。推奨されるキーサイズは、RSA では 1024、ECDSA では 348 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。
- [続行（Continue）] をクリックします。

ステップ 9 [詳細オプション] ステップでは、以下を設定できます。

[失効] タブでは、以下を設定できます。

- [証明書失効リスト（CRL）の有効化）]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布URLを取得するために、[証明書からのCRL配布ポイントの使用] がオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得したCRLをキャッシュすることで、保存制限を超える可能性がある場合は、ASAにより使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

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

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

  [ナンス拡張子を無効化] ：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。使用している OCSP サーバーから、この一致するナンス拡張子を含まない事前に生成した応答を送信する場合は、[ナンス拡張子を無効化] チェックボックスをオフにしてください。

  [評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェックボックスをオンにします。

  失効チェックの詳細については、『Cisco ASA Series General Operations ASDM Configuration、XY』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA 証明書を使用]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。
  - [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。
- [ID証明書の使用]：登録済み ID 証明書の使用方法を指定します。
  - [SSL & IPSec]：SSL & IPSec 接続の認証に使用します。
  - [コード署名者]：コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

- **その他のオプション**：
  - [基本制約拡張でCAフラグを有効化する]：この証明書で他の証明書に署名できるようにする場合はこのオプションをオンにします。基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。証明書におけるこれらの項目のプレゼンス
  - [このCAが発行した証明書を受け入れる]：指定した CA の証明書を ASA で受け入れるようにするにはこのオプションを選択します。
  - [IPsecキーの使用状況を無視]：IPsec リモートクライアント証明書のキーの使用状況および拡張キーの用途拡張の値を検証しない場合は、このオプションを選択します。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、このオプションはイネーブルになっていません。

ステップ 10 [追加（Add）] をクリックします。

これにより、トラストポイント証明書オブジェクトが作成されます。

信頼できる CA 証明書オブジェクトを追加する

外部の認証局から信頼できる CA 証明書を取得するか、自身の内部 CA を使用して（OpenSSL ツールを使用するなど）CA 証明書を作成します。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）

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] > [ASA] > [トラストポイント（Trustpoints）] を選択します。

ステップ 2 証明書の [オブジェクト名（Object Name）] を入力します。名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 3 [証明書タイプ] ステップで、[信頼できる CA 証明書（Trusted CA Certificate）] を選択します。

ステップ 4 [証明書の内容（Certificate Contents] ステップで、証明書の内容をテキストボックスに貼り付けるか、ウィザードの説明に従って CA 証明書ファイルをアップロードします。

ステップ 5 [続行（Continue）] をクリックします。ウィザードの手順が 4 に進みます。

証明書は、次のガイドラインに合致している必要があります。

- 証明書内のサーバ名は、サーバのホスト名またはIPアドレスと一致している必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。
- 証明書は PEM または DER 形式の X509 証明書である必要があります。

- 貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

ステップ 6 [詳細オプション（Advanced Options）] ステップでは、以下を構成できます。

[失効] タブでは、以下の設定を行うことができます。

- [証明書失効リスト（CRL）の有効化）]：CRL の確認を有効にするにはオンにします。

  デフォルトでは、証明書からの失効リスト配布 URL を取得するために、[証明書からの CRL 分散ポイントの使用（Use CRL distribution point from the certificate）] がオンになっています。

  [キャッシュ更新時間（分）]：キャッシュの更新間隔を分単位で指定します。デフォルトは60分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

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

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

  [ナンス拡張子を無効化] ：このチェックボックスをオンにすると、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。使用している OCSP サーバーから、この一致するナンス拡張子を含まない事前に生成した応答を送信する場合は、[ナンス拡張子を無効化] チェックボックスをオフにしてください。

  [評価の優先度]：CRL または OSCP で最初に証明書の失効ステータスを評価するかどうかを指定します。

- [失効情報に到達できない場合は証明書を有効と見なす]：失効情報に到達できない場合に証明書を有効な証明書と見なすには、このチェックボックスをオンにします。

  失効チェックの詳細については、『 Cisco ASA Series General Operations ASDM Configuration、XY』ドキュメントの「基本設定」ブックの「デジタル証明書」の章を参照してください。

[その他] タブをクリックします。

- [検証にCA証明書を使用（Use CA Certificate for the Validation of）]：この CA によって検証できる接続のタイプを指定します。
  - [IPSecクライアント]：リモート SSL サーバーによって提示された証明書を検証します。
  - [SSLクライアント]：着信 SSL 接続によって提示された証明書を検証します。
  - [SSLサーバー]：着信 IPSec 接続によって提示された証明書を検証します。
- **その他のオプション**：
  - [このCAが発行した証明書を受け入れる（Accept certificates issued by this CA）]：指定した CA の証明書を ASA で受け入れるようにするにはこのチェックボックスをオンにします。
  - [このCAの下位CAが発行した証明書を受け入れる（Accept certificates issued by this CA）]：下位 CA の証明書を ASA で受け入れるようにするにはこのチェックボックスをオンにします。
  - [IPsecキーの使用状況を無視（Ignore IPsec Key Usage）]：IPsec リモートクライアント証明書のキーの使用状況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、このオプションを選択します。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、このオプションはイネーブルになっていません。

ステップ 7 [追加（Add）] をクリックします。

これにより、トラストポイント証明書オブジェクトが作成されます。

証明書コンテンツに基づく自己署名済み CSR 証明書の生成

自己署名証明書と CSR 証明書の CN と SANS の内容を理解する必要があります。内容は、作成時に指定したパラメータに基づいています。AnyConnect クライアントが組織の対象となる VPN ヘッドエンドに接続するには、パラメータを正確に設定する必要があります。

このセクションでは、指定されたパラメータに基づいて自己署名証明書と CSR 証明書の内容を理解できるように、さまざまなユースケースと例を示します。

ユースケース 1：異なる CN 値と FQDN 値

例：

- 共通名（CN）：mywebsite.com
- FQDN：mysan.com

表 *4:* 例：異なる *CN* 値と *FQDN* 値

	共通名	unstructuredName	SANS
自己署名	mywebsite.com	mysan.com	mysan.com

	共通名	unstructuredName	SANS
CSR	mywebsite.com	mysan.com	-

ユースケース 2：FQDN フィールドを [なし（None）] に設定

例：

- 共通名（CN）：mywebsite.com
- FQDN：なし（None）

表 *5*：例：*FQDN* フィールドを *[*なし（*None*）*]* に設定

	共通名	SANS
自己署名	ホスト名	-
CSR	mywebsite.com	-

ユースケース 3：FQDN なし（デフォルトの FQDN）

例：

- 共通名（CN）：mywebsite.com

表 *6*：例：*FQDN* なし（デフォルトの *FQDN*）

	共通名	unstructuredName	SANS
自己署名	mywebsite.com	ホスト名	-
CSR	mywebsite.com	ホスト名	ホスト名

ユースケース 4：FQDN で IP アドレスを指定する

例：

- 共通名（CN）：mywebsite.com
- FQDN：4.5.6.7

表 *7*：例：*FQDN* で *IP* アドレスを指定する

	共通名	unstructuredName	SANS
自己署名	mywebsite.com	4.5.6.7	-
CSR	mywebsite.com	4.5.6.7	4.5.6.7

ユースケース 5：IP アドレスを指定する

例：

- IP アドレス：4.5.6.7
- 共通名（CN）：mywebsite.com
- FQDN：fqdn.com

表 *8：*例：*IP* アドレスを指定する

	共通名	unstructuredAddress	unstructuredName	SANS
自己署名	mywebsite.com	4.5.6.7	fqdn.com	-
CSR	mywebsite.com	4.5.6.7	fqdn.com	fqdn.com

ユースケース 6：シリアル番号のチェックボックスがオン

例：

- シリアル番号：9AQXMWOKDT9

表 *9：*例：*IP* シリアル番号のチェックボックスがオン

	serialNumber	SANS
自己署名	9AQXMWOKDT9	-
CSR	9AQXMWOKDT9	fqdn.com

ユースケース 7：メールアドレスを指定する

例：

- EA：abc@xyz.com

表 *10：*例：メールアドレスを指定する

	unstructredName	emailAddress	SANS
自己署名	ホスト名	abc@xyz.com	ホスト名
CSR	ホスト名	abc@xyz.com	-

RA VPN オブジェクト

サービス オブジェクト

ASA サービスオブジェクト

ASA サービスオブジェクト、サービスグループ、およびポートグループは、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。サービスオブジェクトでは、単一のプロトコルを指定して、そのプロトコルを送信元ポート、宛先ポート、または送信元ポートと宛先ポートの両方に割り当てることができます。サービスグループには多くのサービスオブジェクトが含まれ、複数の種類のプロトコルを含めることができます。

ポートグループは、一種の ASA サービスオブジェクトです。ポートグループには、サービスタイプ（TCP や UDP など）と組み合わせるポートオブジェクト、およびポート番号またはポート番号の範囲が含まれます。その後、トラフィックの一致基準を定義するためにセキュリティポリシーでオブジェクトを使用できます。たとえば、これらをアクセス制御ルールで使用して、特定の範囲の TCP ポートへのトラフィックを許可できます。

詳細については、「ASA サービスオブジェクトの作成と編集」を参照してください。

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で識別されます。CDO は、ASA および Firepower（FTD）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（Protocols）」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。CDO は、ASA および Firepower（FTD）が導入準備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。

CDO 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。CDO 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 （11 ページ）

ASA サービスオブジェクトの作成と編集

サービスオブジェクトでは、単一のプロトコルを指定して、そのプロトコルを送信元ポート、宛先ポート、または送信元ポートと宛先ポートの両方に割り当てることができます。

ステップ 1 [オブジェクト] タブをクリックして、[オブジェクト] ページを開きます。

ステップ 2 **[オブジェクトの作成]** > **[ASA]** > **[サービス（Service）]** をクリックします。

ステップ 3 オブジェクト名を入力します。

ステップ 4 [サービスオブジェクトの作成（Create a service object）] を選択します。

ステップ 5 [サービスタイプ（Service Type）] ボタンをクリックし、オブジェクトを作成するプロトコルを選択します。

- TCP、UDP、およびTCP-UDPサービスタイプの場合、送信元ポート、宛先ポート、または両方のポートを入力します。
  - 送信元ポート ID を使用すると、特定の番号のポートから発信されたトラフィックを照合できます。送信元ポートIDで、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
  - 宛先ポートIDを使用すると、特定の番号のポートに到着するトラフィックを照合できます。宛先ポートIDで、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
- **プロトコルサービスタイプの場合**、0 ～ 255 の範囲のプロトコル番号または、ip、tcp、udp、gre などの既知の名前を入力します。

ステップ 6 [追加（Add）] をクリックします。

例

- 着信 FTP トラフィックを識別するサービスオブジェクトは、TCP サービスタイプと 21 の宛先ポート範囲を持つオブジェクトです。
- 発信 DNS および DNS over TCP トラフィックを識別するサービスオブジェクトは、tcp-udb サービスタイプと 53 に等しい送信元ポートを持つオブジェクトです。

ASA サービスグループの作成

サービスグループは、1 つ以上のプロトコルを表す 1 つ以上のサービスオブジェクトで構成できます。

ステップ 1 [オブジェクト（Objects）] タブをクリックして、[オブジェクト（Objects）] ページを開きます。

ステップ 2 **[オブジェクトの作成（Create Object）]** > **[ASA]** > **[サービス（Service）]** をクリックします。

ステップ 3 オブジェクト名を入力します。

ステップ 4 [サービスグループの作成（Create a service group）] を選択します。

ステップ 5 [オブジェクトの追加（Add Object）] をクリックし、オブジェクトを選択して [選択（Select）] をクリックすることで既存のオブジェクトを追加します。このステップを繰り返してさらにオブジェクトを追加します。

ステップ 6 必要に応じて、追加の個別サービスタイプの値をサービスグループに追加します。

- **TCP、UDP、および TCP-UDP サービスタイプの場合、**送信元ポート、宛先ポート、または両方のポートを入力します。
  - 送信元ポート ID を使用すると、特定の番号のポートから発信されたトラフィックを照合できます。送信元ポート ID で、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
  - 宛先ポート ID を使用すると、特定の番号のポートに到着するトラフィックを照合できます。宛先ポート ID で、演算子（等しい、範囲、より小さい、より大きい、または等しくない）を選択し、適切なポート番号または範囲を指定します。
- **プロトコルサービスタイプの場合**、0 ～ 255 の範囲のプロトコル番号または、ip、tcp、udp、gre などの既知の名前を入力します。

ステップ 7 さらに個別のポート値を追加するには、[別の値を追加（Add Another Value）] をクリックして、ステップ 6 を繰り返します。

ステップ 8 サービスグループへのサービスオブジェクトとサービス値の追加が完了したら、[追加] をクリックします。

ASA サービスオブジェクトまたはサービスグループの編集

ステップ 1 [オブジェクト] タブをクリックして、[オブジェクト] ページを開きます。

ステップ 2 オブジェクトをフィルタリングして編集するオブジェクトを見つけ、オブジェクトテーブルでオブジェクトを選択します。

ステップ 3 詳細ペインで、[編集] をクリックします。

ステップ 4 前述の手順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。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 CDO は、変更の影響を受けるポリシーを表示します。[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ポリシーへの変更を確定します。

ASA 時間範囲オブジェクト

時間範囲オブジェクトとは

時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能またはアセットに時間ベースでアクセスするためにネットワークポリシーで使用されます。たとえば、勤務時間中にのみ特定のサーバーへのアクセスを許可するアクセスルールを作成できます。時間範囲を作成してもデバイスへのアクセスは制限されません。これらのオブジェクトに設定される時間は、デバイスのローカル時間であることに注意してください。

このオブジェクトには、絶対時間範囲または反復時間範囲を追加できます。反復時間範囲は、定期的な時間範囲と見なされます。

（注） 1 つの時間範囲に絶対（absolute）値と定期（periodic）値の両方が指定されている場合、periodic 値は absolute の開始時刻に到達した後にのみ評価され、absolute の終了時刻に到達した後は評価されません。

ASA の時間範囲オブジェクトの作成

ASA デバイスの時間範囲オブジェクトを作成するには、次の手順を使用します。

ステップ 1 左側のナビゲーションバーで、[オブジェクト] をクリックします。

ステップ 2 青いプラスボタン 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]** > **[時間範囲]**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 時間範囲を定義します。

- [絶対時間範囲（Absolute Time Range）]：希望する時間範囲の開始時間と終了時間を入力します。このオブジェクトを数分、数時間、数日、または数週間かけて実行することを選択できます。時間範囲オブジェクトには、絶対時間範囲を 1 つだけ指定することができます。
- [定期的な時間範囲（Recurring Time Ranges）]： をクリックして、毎週繰り返される定期的な時間範囲を追加します。ドロップダウンメニューから [頻度（Frequency）]、時間範囲を有効にする [曜日（Days）]、[開始時間（Start）] と [終了時間（End）] を選択します。時間範囲オブジェクトは、複数の周期範囲を持つことができます。

（注） 時間範囲オブジェクトの開始時間と終了時間はオプションです。オブジェクトに開始時間が設定されていない場合、時間範囲はすぐに有効になります。オブジェクトに終了時間が設定されていない場合、時間範囲は無期限に続きます。

ステップ 6 [追加] をクリックしてオブジェクトを作成します。

ASA の時間範囲オブジェクトの編集

ASA デバイスの時間範囲オブジェクトを編集するには、次の手順を使用します。

ステップ 1 左側のナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 オブジェクトをフィルタリングして編集するオブジェクトを見つけ、オブジェクトテーブルでオブジェクトを選択します。

ステップ 3 詳細ペインで、[編集（Edit）] をクリックします。

ステップ 4 必要に応じて値を編集し、[保存（Save）] をクリックします。

ステップ 5 オブジェクトが現在いずれかのポリシーで使用されている場合、CDO は変更の影響を受けるポリシーを表示します。[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ポリシーへの変更を確定します。

ステップ 6 オブジェクトがデバイスのポリシーで使用されている場合は、行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

関連情報：

- オブジェクトの削除
- ASA レガシー ネットワーク ポリシー

セキュリティ ポリシー管理

セキュリティポリシーは、目的の宛先へのトラフィックを許可するか、セキュリティ脅威が特定された場合にトラフィックをドロップすることを最終的な目標として、ネットワークトラフィックを検査します。CDO を使用して、さまざまな種類のデバイスでセキュリティポリシーを設定できます。

- ASA ポリシー（拡張アクセスリスト） （47 ページ）
- ネットワーク アドレス変換 （56 ページ）

ASA レガシー ネットワーク ポリシー

このセクションでは、Cisco Defense Orchestrator（CDO）によって管理されるすべてのデバイスで使用される、あらゆるネットワークポリシーのリストを表示するレガシー ネットワーク ポ

リシーページに関する情報を提供します。**[ポリシー]**>**[ASAポリシー]**を選択して、ネットワークポリシーページに移動します。

ネットワークポリシーは、ネットワークルールのコレクションです。各ネットワークルールは、送信元および接続先の IP アドレス、IP プロトコル、ポート番号、EtherType などの特性に基づいて、ネットワークトラフィックがネットワーク接続先に到達することを許可または阻止します。

CDO はネットワークポリシーを作成するときに、それを ASA インターフェイスに関連付け、ポリシーに 1 つのデフォルトルールを作成します。インターフェイスに関連付けられたネットワークポリシーは、ASA では「アクセスグループ」と呼ばれます。ポリシー名は、ASA のアクセス制御リスト（ACL）名に相当します。CDO が作成したデフォルトのルールと、このネットワークポリシーに追加する後続のルールは、ASA ではアクセス コントロール エントリ（ACE）と呼ばれます。

関連情報：

- レガシービューの ASA ネットワークポリシーの作成
- ASA ネットワークポリシーの編集
- ASA ネットワークポリシーのコピー
- ASA ネットワークポリシーの比較
- ASA ネットワークポリシーの削除
- ASA ネットワークポリシーとルールの検索とフィルタ処理
- 共有 ASA ネットワークポリシー
- アクセス コントロール エントリ（ACE）

レガシービューの ASA ネットワークポリシーの作成

ASA ネットワークポリシーを作成するには、次の手順を実行します。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [デバイス] フィルタをクリックして、ポリシーを保存するデバイスを検索します。

ステップ 4 ポリシーの名前を入力します。1 つのデバイスに同じ名前のネットワークポリシーを 2 つ持つことはできません。

ステップ 5 このポリシーを適用するインターフェイスを選択します。

ステップ 6 ポリシーがアウトバウンドトラフィック用か、インバウンドトラフィック用かを指定します。同じデバイス上の同じ方向の同じインターフェイスに対して 2 つのポリシーを持つことはできません。

ステップ 7 [保存（Save）] をクリックします。CDO は、ネットワークポリシーと、そのポリシーの単一の「permit ip any any」ルールを作成します。

ステップ 8 必要に応じて、ASA ネットワークポリシーの編集。

ステップ 9 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開するか、待機してから複数の変更を同時に展開します。

ASA ネットワークポリシーの編集

Defense Orchestrator を使用すると、ポリシーの詳細ページからネットワークポリシーとポリシールールを編集できます。次の方法で ASA ポリシーを編集できます。

- ポリシーの名前変更
- ポリシーへのルールの追加
- ポリシー内でのルールの移動
- ポリシー間でのルールの移動
- ポリシーのルールの非アクティブ化
- ルールアクティビティのログ記録
- ポリシーの時間範囲の定義

ポリシーの名前変更

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 名前を変更するネットワークポリシーを選択します。

ステップ 3 詳細ペインの名前変更アイコン をクリックします。

ステップ 4 ポリシー名を編集し、青色のチェックボックスをクリックして変更を保存します。

ポリシーへのルールの追加

ステップ 1 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 編集するネットワークポリシーを選択します。

ステップ 3 [ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 詳細ペインで、編集ツールのツールバーの をクリックして、ネットワークポリシーにルールを追加します。ポリシーで強調表示されたルールの上に新しいルールが追加されます。ルールは、ルールのリスト内の位置によって、1 から最後の番号までの順に優先順位付けされます。

（注） 新しいルールには、デフォルトで [許可（Permit）] アクションが割り当てられます。

ステップ 5 [**保存（Save）**] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 6 ポリシーの詳細ペインで [デバイス（Devices ）] フィールドを確認します。エントリの最適数を超えた場合、ASA がインストールされている ASA ハードウェアモデルに応じて、「ACE カウントが超過しました。最大エントリ 500 に対し1000 エントリが見つかりました」のような警告が表示されます。

ステップ 7 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ポリシー内でのルールの移動

ステップ 1 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 ネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 ルールテーブルでルールを選択し、[編集ツール（Edit Tools）] バーで [カット（cut）] をクリックします。

ステップ 5 カットしたルールの後に配置するルールを選択します。ルールは、ルールのリスト内の位置によって優先順位付けされます。ルールの位置が高いほど、優先順位は高くなります。

ステップ 6 [貼り付け（paste）] をクリックします。

ステップ 7 [**保存（Save）**] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 8 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ポリシー間でのルールの移動

あるポリシーのルールをコピーして、別のポリシーに貼り付けることができます。

ステップ 1 **[ポリシー（Policies）] > [ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 コピーするルールを含むネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 ルールテーブルでルールを選択し、[編集ツール（Edit Tools）] バーで [コピー] をクリックします。

ステップ 5 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 6 ルールをコピーするネットワークポリシーを選択します。

ステップ 7 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 8 コピーしたルールの後に配置するルールを選択します。ルールは、ルールのリスト内の位置によって優先順位付けされます。ルールの位置が高いほど、優先順位は高くなります。

ステップ 9 [貼り付け（paste）] をクリックします。

ステップ 10 [保存（**Save**）] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 11 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ポリシーのルールの非アクティブ化

ルールはデフォルトでアクティブです。ポリシー内の個々のルールを非アクティブ化できます。

ステップ 1 [ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 非アクティブ化するルールを含むネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 非アクティブ化するルールを選択します。

ステップ 5 [アクティブ（Active）] 設定をスライドしてオフにします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [保存（**Save**）] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 8 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ルールアクティビティのログ記録

ネットワークポリシールールに起因するアクティビティは、デフォルトではログに記録されません。個別のルールについて、ロギングを有効化できます。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 有効化するルールを含むネットワークポリシーを選択します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 アクティビティをログ記録するルールを選択します。

ステップ 5 スライダをクリックしてログを有効化にします。

ステップ 6 [Edit] をクリックします。

ステップ 7 ロギングレベルと、そのルールからのアクティビティが収集される頻度を選択します。次の表に、syslog メッセージの重大度の一覧を示します。

重大度	説明
emergencies	システムが使用不可能な状態です。
alert	すぐに措置する必要があります。
critical	深刻な状況です。
error	エラー状態です。
warning	警告状態です。
Notification（通告）	正常ですが、注意を必要とする状況です。
informational	情報メッセージです。
debugging	デバッグ メッセージです。
（注）	ASA は、重大度 0（緊急）の syslog メッセージを生成しません。

ステップ 8 ロギング間隔を変更することもできます。ロギング間隔は、間隔中にログがヒットされた回数を示します。ロギング間隔は、1 ～ 600（秒単位）で定義されます。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。

ステップ 9 [**保存（Save）**] をクリックします。Defense Orchestrator によって、変更の影響を受けるデバイスが特定されます。

ステップ 10 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ポリシーの時間範囲の定義

時間ベースの ASA ネットワークポリシーにより、時刻に基づいたネットワークとリソースへのアクセスが許可されます。時刻は、時間範囲オブジェクトによって定義されます。時間範囲オブジェクトには開始時間と終了時間があり、定期的なイベントとして定義することもできます。

時間範囲オブジェクトが ASA ですでに定義されている場合は、それらをネットワークポリシーに関連付けることができます。時間範囲オブジェクトが ASA にまだ存在しない場合は、Defense Orchestrator の CLI ツールを使用して作成するか、ASA で直接作成する必要があります。

次の手順に従って、ネットワークポリシーの時間範囲を追加します。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 編集するネットワークポリシーを選択します。

ステップ 3 [ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 [ネットワークポリシー（Network Policy）] ボックスで、スライダをクリックして時間範囲を有効にします。

ステップ 5 時間範囲オブジェクトを**作成**するか、ドロップダウンリストから既存の時間範囲オブジェクトを**選択**します。

ステップ 6 [**保存（Save**）] をクリックします。

ステップ 7 [デバイスとサービス] ページに戻り、ポリシーを編集したデバイスを選択します。デバイスが同期されていないことがわかります。

ステップ 8 [プレビューして展開...（Preview and deploy..）] をクリックします。

ステップ 9 [デバイスの同期（Device Sync）] ボックスで、ポリシーを作成するコマンドとポリシーのルールを確認します。

ステップ 10 示された変更に問題がない場合は、[デバイスに変更を適用（Apply Changes to Device）] をクリックします。

ステップ 11 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ASA ネットワークポリシーのコピー

この手順を使用して、ある ASA から別の ASA にネットワークポリシーをコピーします。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 コピーするポリシーを検索してフィルタリングします。

ステップ 3 コピーするネットワークポリシーの行で、[コピー] アイコンをクリックします。

ステップ 4 ポリシーをデバイスに追加します。

- **単一のインターフェイスに割り当てられたネットワークポリシーの場合**：[デバイスにポリシーを追加（Add Policy to Device）] ダイアログボックスで、ポリシーをコピーするデバイス、インターフェイス、およびトラフィックの方向を選択します。グローバルアクセスポリシーを別のデバイスにコピーする場合
- **グローバルポリシーの場合**：[デバイスにポリシーを追加（Add Policy to Device）] ダイアログボックスで、ポリシーをコピーするデバイスを選択し、[グローバル ポリシーとして作成（Create as a global policy）] をオンにします。ポリシーのインターフェイスまたは方向を選択できないことがわかります。グローバルポリシーは常にデバイス上のすべてのインターフェイスに割り当てられ、常にインバウンドトラフィックを評価します。

ステップ 5 [**保存（Save**）] をクリックします。

ステップ 6 行った変更を今すぐレビューして展開するか、待機して、複数の変更を同時に展開します。すべてのデバイスの構成変更のプレビューと展開 （178 ページ）

ASA ネットワークポリシーの比較

ステップ 1 ナビゲーションウィンドウで、[ポリシー（Policies）] > [ASAポリシー（ASA Policies）] を選択します。

ステップ 2 ビューアの右上隅にある [比較] をクリックします。

ステップ 3 比較するポリシーを 2 つまで選択します。

ステップ 4 ビューアの下部にある [比較の表示（View Comparison）] をクリックします。これにより、比較ビューアが表示されます。完了したら、[完了（Done）] をクリックし、[比較を完了（Done Comparing）] をクリックします。

ASA ネットワークポリシーの削除

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックして、デバイスを見つけます。

ステップ 3 [ASA] タブをクリックし、ポリシーを削除する ASA を検索して選択します。

ステップ 4 [管理]ペインで、[構成] をクリックします。

ステップ 5 [編集（Edit）] をクリックします。

ステップ 6 デバイス構成で、ネットワークポリシーとルールを探します。

ネットワークポリシーは、ASA 構成ファイルではアクセスグループと呼ばれ、次のようなフォーマットになっています。

```
access-group <ポリシー名> <トラフィックの方向> interface <インターフェイス名>
```

アクセスグループエントリの例を以下に示します。

```
access-group abc-75-1-out out interface interface-1
```

ネットワークルールは、ASA 構成ファイルではアクセスリストと呼ばれ、次のような形式になっています。

```
access-list <ポリシー名> extended permit ip any any
```

アクセスリストエントリの例を以下に示します。

```
access-list abc-75-1-out extended permit ip any any
```

ステップ 7 ネットワークポリシーを含む行とネットワークルールを含む行をハイライトして削除します。

ステップ 8 変更を [保存（Save）] します。

ステップ 9 行った変更を今すぐすべてのデバイスの構成変更のプレビューと展開か、待機してから複数の変更を一度に展開します。

ASA ネットワークポリシーとルールの検索とフィルタ処理

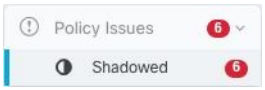
検索バーを使用して、ネットワークポリシーの名前およびポリシー内のルールに含まれる名前、キーワード、またはフレーズを検索します。検索では大文字と小文字が区別されません。

Filter

フィルタサイドバーを使用して、ネットワークポリシーの問題、共有ポリシー、および特定のデバイスのポリシーを見つけます。フィルタリングは。加算的ではなく、各フィルタ設定は互いに独立して機能します。

ポリシーの問題

CDO は、シャドウルールを含むネットワークポリシーを識別します。シャドウルールを含むポリシーの数は、[ポリシーの問題（Policy Issues）] フィルタに示されます。



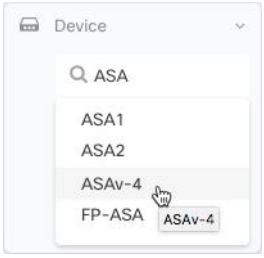
CDO は、ネットワークポリシーページのシャドウバッジ ◑ で、シャドウイングされたルールとそれらを含むネットワークポリシーをマークします。[シャドウイング済み（Shadowed）] をクリックして、シャドウイングされたルールを含むすべてのポリシーを表示します。詳細については、「シャドウイングされたルール」を参照してください。

Shared Policies

共有ポリシーは、複数のデバイスで検出されるポリシーです。共有ポリシーに加えられた変更は、そのポリシーが検出されたすべてのデバイスに影響します。次の例では、**inside-acl-in** ポリシーが 2 つのデバイスで共有されています。詳細については、「共有 ASA ネットワークポリシー」を参照してください。

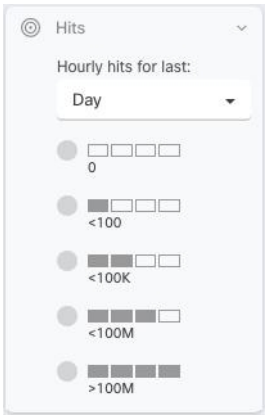
デバイス（Devices）

[デバイス] フィルタを展開し、[デバイスの検索（Search devices）] フィールドに名前または IP アドレスを入力して、ネットワークポリシーリストをデバイスでフィルタリングし、結果内で見つかったデバイスを選択します。



ヒット数（Hits）

このフィルタを使用して、指定された期間に何度もトリガーされたデバイスを対象にしてポリシーを特定します。



ヒットがゼロのネットワークポリシーを見つける

ヒットのないネットワークポリシーがある場合は、ネットワークポリシーを編集してより効果的にするか、単に削除することができます。

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 [フィルタ（Filter）] ペインで [すべて表示（Show All）] をクリックして、既存のフィルタをすべてクリアします。

ステップ 3 [ヒット（Hits）] フィルタを展開します。

ステップ 4 期間を選択します。

ステップ 5 0 ヒットを選択します。

ヒットがゼロのデバイス上のすべてのネットワークポリシーを見つける

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 [フィルタ（Filter）] ペインで [すべて表示（Show All）] をクリックして、既存のフィルタをすべてクリアします。

ステップ 3 [デバイス] フィルタを展開し、フィルタを適用するデバイスを選択します。
ステップ 4 [ヒット（Hits）] フィルタを展開します。
ステップ 5 期間を選択します。
ステップ 6 0 ヒットを選択します。

ネットワークポリシー内のルールがヒットする頻度の検索

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。
ステップ 2 [フィルタ（Filter）] ペインで [すべて表示（Show All）] をクリックして、既存のフィルタをすべてクリアします。
ステップ 3 1 つのデバイスで使用されるネットワークポリシーを選択します。
ステップ 4 ルールテーブルの [ヒット（Hits）] 列を調べて、ネットワークポリシーの各ルールがヒットしている頻度を確認します。
ステップ 5 ネットワークポリシーのルールが多すぎて結果を一目で確認できない場合は、[ヒット（Hits）] フィルタを展開します。
ステップ 6 期間を選択します。
ステップ 7 各種のヒットフィルタを選択して、各種のルールがどのカテゴリに分類されるかを確認します。

共有ネットワークポリシーがヒットする頻度の検索

ネットワークポリシーのヒット数は、個々のデバイスに対して計算されます。フィルタでデバイスを指定しないと、2 つ以上のデバイスで共有されている 1 つのネットワーク ポリシーのヒット率を表示できません。

ステップ 1 **[ポリシー（Policies）]** > **[ASAアクセスポリシー（ASA Access Policies）]**に移動します。
ステップ 2 ポリシーテーブルの上にある [クリア] をクリックして、既存のフィルタをクリアします。
ステップ 3 [共有ポリシー（Shared Policies）] フィルタを展開し、[共有（Shared）] をクリックします。
ステップ 4 共有されているネットワークポリシーを選択します。
ステップ 5 そのポリシーの詳細ペインで、そのネットワークポリシーを使用しているデバイスをメモしてから、ネットワーク ポリシー テーブルに戻ります。
ステップ 6 共有されているポリシーの名前を検索フィールドに入力します。
ステップ 7 [デバイス] フィルタを展開し、共有されているポリシーを使用しているいずれかのデバイスでフィルタします。
ステップ 8 [ヒット（Hits）] フィルタを展開します。
ステップ 9 期間を選択します。
ステップ 10 各種のヒットフィルタを選択して、ポリシーがどのカテゴリに分類されるのかを確認します。

ヒット率によるネットワークポリシーのフィルタ処理

ステップ 1 **[ポリシー（Policies）] > [ASAアクセスポリシー（ASA Access Policies）]** に移動します。

ステップ 2 ポリシーテーブルの上にある [クリア] をクリックして、既存のフィルタをクリアします。

ステップ 3 [ヒット（Hits）] フィルタを展開します。

ステップ 4 期間を選択します。

ステップ 5 異なるヒット率カテゴリを選択します。CDO は、指定したレートでヒットしているポリシーを表示します。ヒットレートの基準に一致する共有ネットワークポリシーがある場合、CDO は、共有ポリシーを使用するすべてのデバイスの行を表示します。

共有 ASA ネットワークポリシー

Cisco Defense Orchestrator（CDO）は、複数の ASA によって使用される同一のネットワークポリシーを見つけ、ネットワークポリシーページでそれらを識別します。共有ネットワークポリシーがある場合は、一度変更して、ポリシーを共有する他のデバイスに変更を配布できます。これにより、デバイス間でネットワークポリシーの一貫性が保たれます。

共有ネットワークポリシーの属性

ネットワーク ポリシー テーブルは、ネットワークポリシーを使用するデバイスの数を示します。複数のデバイスで使用されることを示すネットワークポリシーは、共有ポリシーです。共有ネットワークポリシーを検索するには、次の手順に従います。

ステップ 1 **[ポリシー（Policies）] > [ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 フィルタペインで、[すべて表示（Show All）] をクリックして、ページから過去のフィルタ条件または検索条件をクリアします。

ステップ 3 フィルタバーで、[共有ポリシー（Shared Policies）] を展開して [共有（Shared）] を選択します。

ステップ 4 検索バーにキーワードを入力して、さらに検索を絞り込みます。

ステップ 5 ネットワーク ポリシー テーブルから共有ネットワークポリシーを選択します。

（注） フィルタ条件と検索条件は組み合わせて使用されず、一度に1つしか使用できません。たとえば、「共有ポリシー（Shared Policies）」でフィルタリングすると、すべての共有ポリシーが表示されます。特定のデバイス名を検索に追加すると、ポリシーが共有されているかどうかに関係なく、そのデバイス名で使用されているすべてのネットワークポリシーが表示されます。

共有ネットワークポリシーの編集

ステップ 1 編集する共有 ASA ネットワークポリシー。

ステップ 2 共有ポリシーを選択します。CDO は、CDO 管理対象のどのデバイスがそのネットワークポリシーを使用するかを識別します。

ステップ 3 詳細ペインで、[ポリシーの編集（Edit Policy）] をクリックします。

ステップ 4 ポリシーのルールを編集します。

ステップ 5 [**保存（Save**）] をクリックします。

ステップ 6 [確認（Confirm）] で、変更の影響を受けるデバイスを確認します。

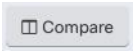
ステップ 7 [デバイスとサービス] ページを開いて、デバイスが同期されていないことを確認します。

ステップ 8 [変更を手動で展開...（Deploy Changes Manually...）] をクリックして、表示される指示に従って、ASA に保存されている設定を更新して変更を反映します。

共有ネットワークポリシーの比較

共有ネットワークポリシーを比較する目的は、少しだけ相違しているポリシーを探し、それらを再調整することです。ほとんど同じポリシーがいくつかある場合、それらは分岐したものであり、実際には同一のポリシーである可能性があります。ネットワークポリシーを再調整すると、CDO はポリシーを共有ポリシーとして認識します。ポリシーを変更する場合、そのポリシーを使用して他のデバイスに変更を配信できるようになります。

ステップ 1 比較する共有 ASA ネットワークポリシー。

ステップ 2 [比較] 

をクリックします。

ステップ 3 比較するネットワークポリシーを 2 つ選択し、[比較の表示（View Comparison）] をクリックします。

ステップ 4 違いをメモし、[比較を終了（Done Comparing）] をクリックします。

ステップ 5 ポリシーの 1 つを変更して他のポリシーと一致させる場合は、ネットワーク ポリシー テーブルからポリシーを選択し、詳細ペインで [ポリシーの編集（Edit Policy）] をクリックして編集します。

ASA ポリシー（拡張アクセスリスト）

Cisco Defense Orchestrator（CDO）は、ネットワークとアプリケーションのセキュリティポリシーをすべてのデバイスで一貫した状態に保つ機能をユーザーに提供します。この独自の機能により、複数のデバイスで同時にポリシーをシンプルかつ簡単に変更できます。

アクセス コントロール エントリ（ACE）

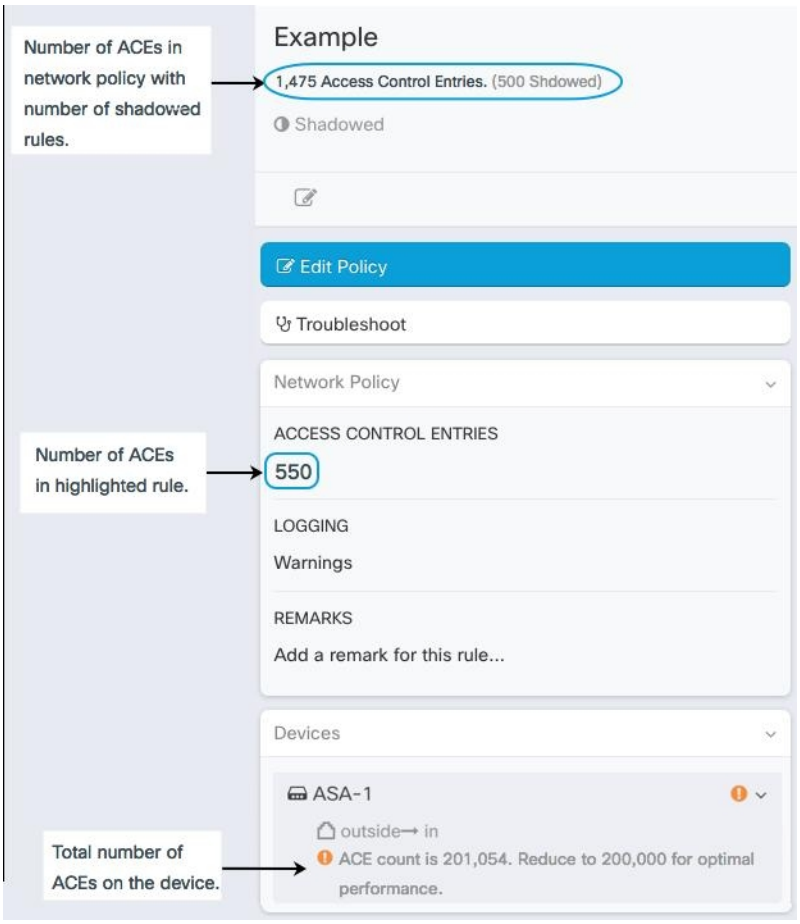
アクセス コントロール エントリについて、確認できるものと確認できないものについて考えてください。

確認できるものは、次のとおりです。CDO のユーザーインターフェイスに関しては、ネットワークポリシーに追加するルールは、ASA のアクセス コントロール エントリです。このルールでは、送信元アドレスと宛先アドレスの間、またはあるアドレスグループと別のアドレスグループの間で許可されるネットワークトラフィックを定義します。

確認できないものは、次のとおりです。ASA は、作成したネットワークルールを拡張して、そのネットワークルールによって暗示される送信元 IP アドレスと宛先 IP アドレスの可能なすべての組み合わせを考慮します。たとえば、1 つのネットワークオブジェクトの 3 つの IP アドレスが別のオブジェクトの 3 つの IP アドレスにアクセスすることを拒否するルールがある場合、ASA がメモリに格納する可能性のあるアクセス コントロール エントリは 9 つあります。

ASA が処理できる ACE の数にハードコードされた制限はありませんが、ACE の数が多すぎると、ASA のパフォーマンスが低下します。特定の ASA デバイスに予想される ACE エントリの最大数については、「Adaptive Security Appliance FAQ」 の表 4「Maximum Access Control Entries for Cisco ASA Models」を参照してください。

CDO は、すべてのネットワークポリシーから派生した ACE の総数を維持し、その ACE 数がアプライアンスで予想される ACE の最大制限数を超えると通知します。CDO が提供する情報は次のとおりです。



デバイス上の ACE 数の削減

予想される ACE の最大数を超えたデバイス上の ACE 数を減らすためのいくつかのアプローチを次に示します。

- 部分的なシャドウルールと完全なシャドウイングされたルールを持つポリシーを探します。必要に応じて、これらのルールを削除します。
- ネットワークポリシーをフィルタリングして、ヒットがゼロのデバイス上のすべてのネットワークポリシーを見つけるか、ヒットがゼロのネットワークポリシー内のルールがヒットする頻度の検索。該当する場合は、ヒットがゼロのポリシーまたはルールを削除します。
- 予想されるアクセス コントロール エントリ数を超えたASA ネットワークポリシーとルールの検索とフィルタ処理て、それらのポリシーを確認します。それらのポリシーの送信元と宛先のアドレス指定を、当初の計画どおりに広くする必要があるかどうかを検討してください。

ASA グローバルアクセスポリシーの設定

グローバルアクセスポリシーは、ASA のすべてのインターフェイスに適用されるネットワークポリシーです。これらのポリシーは、着信ネットワークトラフィックにのみ適用されます。一連のルールをすべての ASA インターフェイスに一様に適用する場合は、グローバルアクセスポリシーを作成します。

1 つの ASA に設定できるグローバルアクセスポリシーは 1 つだけです。他のポリシーと同様に、グローバルアクセスポリシーには複数のルールを割り当てることができます。

ASA グローバルアクセスポリシーは、特定のインターフェイスのネットワークポリシーの後、すべてのトラフィックの暗黙の拒否ルールの前に処理されます。ASA でのルール処理の順序は、次のとおりです。

1. インターフェイス アクセス規則。
2. ブリッジ グループ メンバーのインターフェイスでは、ブリッジ仮想インターフェイス（BVI）のアクセス ルール
3. グローバル アクセス ルール
4. 暗黙的な拒否

ASA グローバルアクセスポリシーの設定に関する制限事項

CDO では、ASA のグローバルアクセスポリシーを作成および編集できます。ただし、CDO に ASA を導入準備したときに ASA にグローバルアクセスポリシーが存在している場合、次の制限があります。

- ポリシーを編集することはできますが、デバイスごとに許可されるグローバルアクセスポリシーは 1 つしかないため、新しいポリシーを作成することはできません。
- ASA のグローバルアクセスポリシーに、CDO がサポートしていないルールが含まれている場合、そのポリシーを編集することはできません。
- ポリシーを削除するには、CLI インターフェイスを使用するか、デバイス構成ファイルを編集する必要があります。

グローバルアクセスポリシーの作成

ステップ 1 **[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** をクリックします。

ステップ 2 フィルタパネルで、ポリシーリストをフィルタ処理して、グローバルポリシーを追加するデバイスを見つけます。

ステップ 3 [ネットワークポリシー（Network Policies）] テーブルの [インターフェイス（Interfaces）] 列で、「グローバル（global）」というラベルの付いたポリシーがないことを確認します。

ステップ 4 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 5 [デバイス] ボタンをクリックし、グローバルポリシーを追加する ASA を選択します。[選択（Select）] をクリックします。

ステップ 6 ポリシーに名前を付け、[グローバルポリシーとして作成（Create as a global policy）] をオンにします。ポリシーのインターフェイスまたは方向を選択できないことがわかります。グローバルポリシーは常にデバイス上のすべてのインターフェイスに割り当てられ、常にインバウンドトラフィックを評価します。

ステップ 7 [保存（**Save**）] をクリックします。

ステップ 8 [ASAネットワークポリシーの編集（Edit an ASA Network Policy）] を使用して、新しいポリシーにルールを追加します。ASA ネットワークポリシーの編集 （37 ページ）

グローバルアクセスポリシーの編集

上記の構成の制限に留意し、[ASAネットワーク ポリシーの編集] を使用してグローバルアクセスポリシーを編集します。ASA ネットワークポリシーの編集 （37 ページ）

（注） [ポリシーの編集] ボタンが非アクティブになっているためにグローバルポリシーを編集できない場合は、ポリシーが ASA で作成され、CDO がサポートしていないオブジェクトを持つルールが含まれている可能性があります。これらのルールは、グローバル アクセス ポリシー テーブルでは表示されません。この場合、CDO の CLI ツールを使用して構成ファイルを編集する必要があります。これには CDO を使用して ASA の構成ファイルを編集するか、ASA で直接グローバルポリシーを編集します。

グローバルアクセスポリシーを別のデバイスにコピーする

[ASAネットワークポリシーのコピー] を使用して、グローバルアクセスポリシーを 1 つのデバイスから別のデバイスにコピーするか、グローバルアクセスポリシーを 1 つのデバイスから別のデバイスの単一のインターフェイスにコピーします。ASA ネットワークポリシーのコピー （41 ページ）

グローバルアクセスポリシーの削除

CDO のユーザーインターフェイスを使用してグローバルアクセスポリシーを削除することはできません。グローバルアクセスポリシーを削除するには、CDO の CLI ツールを使用してコマンドラインでグローバルアクセスポリシーを削除する必要があります。これには CDO を使用して ASA の構成ファイルを編集するか、ASA で直接グローバルポリシーを編集します。

ヒット率

CDO を使用すると、ポリシーの安全でスケーラブルなオーケストレーションに加えて、ポリシールールの結果を評価できるようになり、より正確なポリシー分析のためのシンプルな視覚

化と、根本原因への迅速で実行可能なピボットを、すべてクラウドから1つのペインで行うことが可能になります。ヒット率機能を使用すると、次のことが可能になります。

- 古く照合されないポリシールールを排除し、セキュリティ態勢を強化します。
- ボトルネックを即座に特定し、正確で効率的な優先順位付けを確実に実施することにより、ファイアウォールのパフォーマンスを最適化します（たとえば、トリガーされたポリシールールの優先順位が高くなります）。
- デバイスまたはポリシールールがリセットされた場合でも、設定されたデータ保持期間（1年）の間、ヒット率情報の履歴を維持します。
- 実用的な情報に基づいて、疑わしいシャドウおよび未使用のルールの検証を強化します。更新または削除についての疑問を解消します。
- 事前定義された時間間隔（日、週、月、年）と実際のヒットのスケール（ゼロ、>100、>100k など）を活用して、ポリシー全体のコンテキストでポリシールールの使用を視覚化し、ネットワークを通過するパケットへの影響を評価します。

ASA ポリシーのヒット率の表示

ステップ 1 CDO メニューバーから **[ポリシー（Policies）]** > **[ASAアクセスポリシー（ASA Access Policies）]** を選択します。

ステップ 2 フィルタアイコンをクリックして、開いた状態でピン留めします。

ステップ 3 [ヒット（Hits）]領域で、さまざまなヒットカウントフィルタをクリックして、他のポリシーよりもヒットの頻度が高いポリシーや低いポリシーを表示します。

ネットワークポリシールールのエクスポート

各 Access-Group または Crypto-Map の内容を .csv ファイルにエクスポートできます。この .csv には、各アクセス制御リスト（ACL）と、各 ACL について CDO が持つデータが表示されます。

ステップ 1 ナビゲーションウィンドウで、**[ポリシー（Policies）]** > **[ASAポリシー（ASA Policies）]** を選択します。

ステップ 2 （任意）ASA ネットワークポリシーとルールの検索とフィルタ処理を使用して結果をフィルタ処理します。

ステップ 3 結果からネットワークポリシーを選択します。

ステップ 4 [CSVにエクスポート（Export to CSV）] 

をクリックします。

ステップ 5 CDO は、画面に表示されているルールを .csv ファイルにエクスポートします。

ASA ポリシー変更のデバイスへの適用

Cisco Defense Orchestrator（CDO）でセキュリティポリシーを変更すると、影響を受けるデバイスまたはサービスに変更がステージングされるため、設定が [非同期] になります。現在 [非同期] のデバイスやサービスで [デバイスに展開...（Deploy to Device...）] をクリックすると、ポリシーの変更を確認して適用することができます。

スクリプトによるデバイスの展開

ASAデバイスポリシー構成の変更が完了したら、変更を確認してデバイスに適用する必要があります。

ステップ 1 [デバイス] タブに移動し、[デバイス] タブをクリックします。

ステップ 2 適切なデバイスタイプのタブをクリックし、変更したデバイスをテーブルから選択します。構成ステータスには、デバイスにまだ適用されていない変更があることを示す [非同期] が表示されます。

ステップ 3 右側のサイドバーから [同期] をクリックし、デバイスと CDO 構成を同期済みステータスにするために、デバイスに適用するコマンドを生成します。

ステップ 4 プロンプトが表示されたら、[コマンドのダウンロード] をクリックして、コマンドのコピーをローカルにダウンロードします。これらのコマンドはテキストファイルに含まれており、適用する前に確認できます。必要に応じて変更を元に戻すためのコマンドも生成されます。

ステップ 5 CDOの外部で、標準プロトコルを使用してデバイスにログインし、ダウンロードしたコマンドを適用します。

ステップ 6 すべてのコマンドを入力したら、CDO に戻り、[デバイス] タブで変更されたデバイスを再度選択します。

ステップ 7 [更新] をクリックして、CDO との同期を確認します。

コマンドの一部が実行された場合、または追加のコマンドがアウトオブバンドで実行された場合、CDO は相違点を示すウィンドウを開いて相違点を示し、[競合検出] というステータスに更新することでユーザーに警告します。

ASA ポリシーのセキュリティグループタグ

アクセス制御ルール内で、セキュリティ グループ オブジェクト グループ（以下「SGT グループ」と呼ぶ）のセキュリティグループタグを使用する ASA を導入準備する場合、Cisco Defense Orchestrator では、これらの SGT グループを使用するルールを編集し、そのルールを持っているポリシーを管理できます。ただし、SGT グループを作成したり、CDO GUI を使用して編集したりすることはできません。SGT グループを作成または編集するには、ASA の Adaptive Security Device Manager（ASDM）、または CDO で使用可能なコマンド ライン インターフェイスを使用する必要があります。

CDO のオブジェクトページで SGT グループの詳細を読むと、それらのオブジェクトが編集不可のシステム提供オブジェクトとして識別されていることがわかります。

CDO管理者は、SGTグループを含むACLおよびASAポリシーで次のタスクを実行できます。

- CDO 管理者は、接続先および宛先セキュリティグループを除き、ACL のすべての側面を編集できます。
- SGT グループを含むポリシーを 1 つの ASA から別の ASA にコピーします。

コマンド ライン インターフェイスを使用して Cisco TrustSec を設定する手順の詳細については、お使いの ASA リリースの『ASA CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide』の「ASA and Cisco TrustSec」の章を参照してください。

シャドウイングされたルール

シャドウイングされたルールを含むネットワークポリシーは、ポリシーの少なくとも 1 つのルールがトリガーされることがないポリシーです。これは、それに先行するルールによって、シャドウイングされたルールによるパケットの評価が妨げられるためです。

たとえば、「example」ネットワークポリシーの次のネットワークオブジェクトとネットワークルールについて考えてみます。

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100

access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

次のルールによって評価されるトラフィックはありません

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

その理由は、先行するルール

```
access-list example extended deny ip any4 object 02-50
```

が、10.10.10.2 から 10.10.10.50 の範囲の任意アドレスから到達するすべて IPOv4 アドレスを拒否するためです。

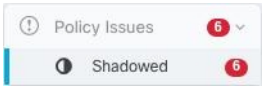
シャドウイングされたルールを持つネットワークポリシーを見つける

シャドウイングされたルールを持つネットワークポリシーを見つけるには、ネットワーク ポリシー フィルタを使用します。

ステップ 1 ナビゲーションウィンドウで、**[ポリシー]** > **[ASAポリシー]**を選択します。

ステップ 2 ASA アクセスポリシーテーブルの上部にあるフィルタアイコンをクリックします。

ステップ 3 [ポリシーの問題] フィルタで、[シャドウイング] をオンにして、シャドウイングされたルールを持つすべてのポリシーを表示します。



シャドウルールを使用した問題の解決

次に示すのは、CDO が前述の「例」のネットワークポリシーで説明されているルールを表示する方法です。

1 行目のルールは、ポリシー内の別のルールをシャドウしているため、シャドウ警告バッジ ⚠ のマークが付いています。2 行目のルールは、ポリシー内の別のルールによってシャドウされているため ◑ マークが付いています。2 行目のルールのアクションは、ポリシー内の別のルールによって完全にシャドウされているためグレー表示されています。CDO は、2 行目のルールをシャドウするポリシー内のルールを通知できます。

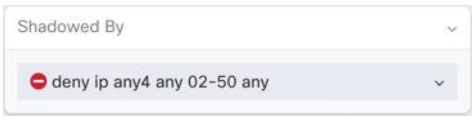
3 行目のルールは、時々のみトリガーできます。これは部分的なシャドウルールです。10.10.10.2 ～ 10.10.10.50 の範囲の IP アドレスに到達しようとする IPv4 アドレスからのネットワークトラフィックは、最初のルールによってすでに拒否されているため、評価されません。ただし、10.10.10.51 ～ 10.10.10.100 の範囲のアドレスに到達しようとする IPv4 アドレスは、最後のルールによって評価され、許可されます。

⚠

注意 CDO は、部分的なシャドウルールにシャドウ警告バッジ ⚠ を適用しません。

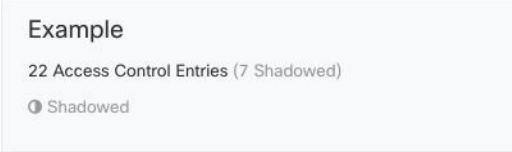
ステップ 1 ポリシーでシャドウルールを選択します。前述の例では、2 行目をクリックすることを意味します。

ステップ 2 ルールの詳細ペインで、[シャドウ基準（Shadowed By）] 領域を探します。この例では、2 行目のルールの [シャドウ基準（Shadowed By）] 領域は、1 行目のルールによってシャドウされていることを示しています。



ステップ 3 シャドウイングルールを確認します。広すぎる場合、シャドウルールを確認します。不要な場合、シャドウルールを編集するか、シャドウルールを削除します。

（注） シャドウルールを削除することで、ASA のアクセス コントロール エントリ（ACE）の数を減らすことができ、他の ACE で他のルールを作成するためのスペースが解放されます。CDO は、1 つのネットワークポリシーのすべてのルールから派生した ACE の数を計算し、ネットワークポリシーの詳細ペインの上部に合計を表示します。ネットワークポリシーのいずれかのルールがシャドウされている場合は、その数もリストされます。



CDO は、ネットワークポリシーの 1 つのルールから派生した ACE の数も表示し、その情報をネットワークポリシーの詳細ペインに表示します。リストの例を次に示します。

ステップ 4 ネットワークポリシーの詳細ペインの [デバイス（Devices）] 領域を調べて、ポリシーを使用するデバイスを特定します。

ステップ 5 [デバイスとサービス（Devices & Service）] ページを開き、ポリシー変更の影響を受けるデバイスに**変更を展開**し直します。

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 の他の機能は、次のとおりです。

- 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。

Cisco Defense Orchestrator 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 NAT ルールおよび Twice NAT ルールは、3 セクションに分割される 1 つのテーブルに保存されます。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 *11 : 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 （60 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 （59 ページ）を参照してください。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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 フィルタと 検索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 （12 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すべてのデバイスの構成変更のプレビューと展開するか、待機してから複数の変更を同時に展開します。

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 （61 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 （63 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 （64 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 （69 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、「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」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」を参照してください。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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] 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] 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 Firepower Threat Defense（FTD）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 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ルールを展開し、FTD の場合はアクセス コントロール ポリシールールを展開して、*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すべてのデバイスの構成変更のプレビューと展開か、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

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD 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 servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

この手順によって作成される *NAT* ルール：

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

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。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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] 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] をクリックします。

ステップ 7 セクション 1 の [タイプ] で、[ダイナミック] 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] 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 Firepower Threat Defense（FTD）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すべてのデバイスの構成変更のプレビューと展開か、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

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD 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、

「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」「」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

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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] をクリックします。

ステップ 7 セクション 1 の [タイプ] 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 Firepower Threat Defense（FTD）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 12 [**保存（Save）**] をクリックします。NAT テーブルの NAT ルールの処理命令 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すべてのデバイスの構成変更のプレビューと展開か、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

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD 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 ftp-object
host 10.1.2.27
```

この手順によって作成される *NAT* ルール

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

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、「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」「」を参照してください。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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] をクリックします。

ステップ 7 セクション 1 の [タイプ] 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] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）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 12 [**保存**（**Save**）] をクリックします。NAT テーブルの NAT ルールの処理命令 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すべてのデバイスの構成変更のプレビューと展開か、待機して、複数の変更を同時に展開します。

ASA の保存済み設定ファイルのエントリ

この手順の結果として ASA の保存済み設定ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD 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 http-object
host 10.1.2.28
```

この手順によって作成される *NAT* ルール

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

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、「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」「」を参照してください。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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] をクリックします。

ステップ 7 セクション 1 の [タイプ] 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 Firepower Threat Defense（FTD）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 12 [保存（**Save**）] をクリックします。NAT テーブルの NAT ルールの処理命令 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すべてのデバイスの構成変更のプレビューと展開するか、待機してから複数の変更を同時に展開します。

ASA の保存済み構成ファイルのエントリ

この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリを次に示します。

（注） これは FTD 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 smtp-object
host 10.1.2.29
```

この手順によって作成される *NAT* ルール

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

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。

ASA の場合、「元のアドレス」プール（変換するプライベート IP アドレスプール）は、アドレス範囲を持つ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、またはプール内のすべてのアドレスを含むネットワークグループにすることができます。FTDの場合、「元のアドレス」プールは、サブネットを定義するネットワークオブジェクト、またはプール内のすべてのアドレスを含むネットワークグループにすることができます。

（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、「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」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。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] 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] 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] 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] をクリックします。

ステップ 7 セクション 1 の [タイプ] で [ダイナミック] を選択し、[続行] 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] で、送信元インターフェイスを [内部] に設定し、接続先インターフェイスを [外部] 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] で、以下のタスクを実行します。

- [元アドレス] で、[選択] 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] で、[選択] 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] はスキップしてください。

ステップ 11 Firepower Threat Defense（FTD）の場合、セクション 5 の [名前] に NAT ルールの名前を入力します。

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すべてのデバイスの構成変更のプレビューと展開か、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

以下は、この手順の結果として ASA の保存済み構成ファイル内に表示されるエントリです。

（注） これは FTD 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 outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

この手順によって作成される *NAT* ルール

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

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、『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』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。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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] 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 Firepower Threat Defense（FTD）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 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すべてのデバイスの構成変更のプレビューと展開か、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

以下は、この手順の結果として ASA の保存済み構成ファイル内に作成および表示されるエントリです。

（注） これは FTD 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 Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

この手順によって作成される *NAT* ルール

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

仮想プライベートネット ワークの管理

バーチャルプライベートネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介してエンドポイント間の安全なトンネルを確立します。

このセクションは、適応型セキュリティアプライアンス（ASA）デバイスのリモートアクセスおよびサイト間 VPN に適用されます。 また、ASA で VPN 接続を構築し、リモートでアクセスするために使用する SSL 標準についても説明します。

CDO は以下のタイプの VPN 接続をサポートします。

- サイト間仮想プライベートネットワーク
- リモートアクセス仮想プライベートネットワーク

サイト間仮想プライベートネットワーク

サイト間 VPN トンネルは、地理的に異なる場所にあるネットワークを接続します。CDO に導入準備された ASA デバイスに存在するサイト間設定のみを監視できます。現在、CDO では、ASA デバイスでサイト間 VPN 設定を構成できません。ただし、デバイスが CDO に導入準備されている場合は、構成を監視できます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコルスイートとインターネット キー エクスチェンジ バージョン 2（IKEv2）を使用して構築されます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。

関連情報：

- ASA サイト間仮想プライベートネットワークのモニタリング

ASA サイト間仮想プライベートネットワークのモニタリング

CDO を使用すると、導入準備 ASA デバイスで既存のサイト間 VPN 設定を監視できます。サイト間の設定は変更も削除もできません。

サイト間 VPN トンネルの接続の確認

[接続の確認（Check Connectivity）] ボタンを使用して、トンネルに対するリアルタイムの接続確認をトリガーし、トンネルの現在の状態（アクティブまたはアイドル）を確認します。サイト間 VPN トンネルの検索とフィルタ処理 （77 ページ）[オンデマンド接続確認（on-demand connectivity check）] ボタンをクリックしていない場合、導入準備されているすべてのデバイスで利用可能なすべてトンネルに対する確認が 1 時間に一度実行されます。

（注）
- CDO は、トンネルがアクティブかアイドルかを判断するために、ASA および FTD で次の接続確認コマンドを実行します。

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- ASA モデルデバイストンネルは常に [アイドル（Idle）] と表示されます。

[VPN] ページからトンネル接続を確認するには、次の手順を実行します。

ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN] をクリックします。

ステップ 2 サイト間 VPN トンネルのトンネルのリストをサイト間 VPN トンネルの検索とフィルタ処理して、選択します。

ステップ 3 右側の [アクション] ペインで、[接続の確認（Check Connectivity）] をクリックします。

VPN の問題の特定

CDO は、ASA デバイスおよび FTD デバイスでの VPN の問題を特定できます（この機能は、AWS VPC サイト間 VPN トンネルではまだ利用できません）。この記事では次のことを説明します。

- ピアが欠落している VPN トンネルを見つける
- 暗号化キーの問題がある VPN ピアを見つける
- トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける
- トンネル設定の問題を見つける

トンネル設定の問題の解決 （76 ページ）

ピアが欠落している *VPN* トンネルを見つける

「Missing IP Peer」状態は、FTD デバイスよりも ASA デバイスで発生する可能性が高くなります。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[サイト間 VPN（Site-to-Site VPN）]**をクリックして VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 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。

ステップ 4 検出された問題を確認します。

ステップ 5 問題を報告している各デバイス▲を選択し、右側の [ピア（Peers）] ペインを確認します。1 つのピア名がリストされます。CDO は、他のピア名を「[Missing peer IP.]」として報告します。

暗号化キーの問題がある *VPN* ピアを見つける

このアプローチを使用して、以下のような暗号化キーの問題がある VPN ピアを見つけます。

- IKEv1 または IKEv2 キーが無効、欠落しているか、一致しない
- トンネルが古くなっているか、暗号化レベルが低い

ステップ 1 CDO ナビゲーションバーで、[VPN] > [サイト間VPN] をクリックして VPN ページを開きます。 >

ステップ 2 [テーブルビュー] を選択します。

ステップ 3 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。

ステップ 4 問題を報告している各デバイス ▲ を選択し、右側の [ピア] ペインを確認します。ピア情報には、両方のピアが表示されます。

ステップ 5 いずれかのデバイスの [ピアの表示] をクリックします。

ステップ 6 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ 7 下部の [トンネルの詳細] パネルで [キー交換] をクリックします。両方のデバイスを表示して、そこでキーの問題を診断できます。

トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける

「アクセスリストが不完全または正しく設定されていない」状態は、ASA デバイスでのみ発生する可能性があります。

ステップ 1 CDO ナビゲーションバーで、[VPN] > [サイト間VPN] をクリックして VPN ページを開きます。 >

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 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。

ステップ 4 問題を報告している各デバイス⚠を選択し、右側の [ピア（Peers）] ペインを確認します。ピア情報には、両方のピアが表示されています。

ステップ 5 いずれかのデバイスの [ピアの表示（View Peers）] をクリックします。

ステップ 6 ダイアグラムビューで、問題を報告しているデバイスをダブルクリックします。

ステップ 7 下部の [トンネルの詳細] パネルで [トンネルの詳細] をクリックします。「ネットワークポリシー：不完全（Network Policy: Incomplete）」というメッセージが表示されます。

トンネル設定の問題を見つける

トンネル設定のエラーは、次のシナリオで FTD デバイスで発生する可能性があります。

- サイト間 VPN インターフェイスの IP アドレスが変更されたときの、「ピア IP アドレス値が変更されました（Peer IP Address Value has changed）」。
- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません（IKE value Mismatch）」というメッセージが表示されます。

ステップ 1 CDO ナビゲーションバーで、[VPN] > [サイト間VPN] をクリックして VPN ページを開きます。 >

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 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。

ステップ 4 [トンネルの問題（Tunnel Issues）] で、[検出された問題（Detected Issues）] をクリックして、エラーを報告している VPN 設定を表示します。問題を報告している（⚠）設定を表示できます。

ステップ 5 問題を報告している VPN 設定を選択します。

ステップ 6 右側の [ピア（Peers）] ペインに、問題のあるピアに⚠アイコンが表示されます。⚠アイコンにカーソルを合わせると、問題と解決策が表示されます。

次のステップ：トンネル設定の問題の解決。

トンネル設定の問題の解決

この手順では、次のトンネル設定の問題を解決を試みます。

- サイト間 VPN インターフェイスの IP アドレスが変更れたときの、「ピア IP アドレス値が変更されました（Peer IP Address Value has changed）」。
- VPN トンネルの IKE 値が他の VPN トンネルと一致しない場合、「IKE 値が一致しません（IKE value Mismatch）」というメッセージが表示されます。

詳細については、「トンネル設定の問題を見つける」を参照してください。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、問題を報告している VPN 設定に関連付けられているデバイスを選択します。

ステップ 4 [競合検出（Conflict Detected）] ステータスの解決。

ステップ 5 CDO ナビゲーションウィンドウで、**[VPN]** > **[サイト間VPN]**をクリックして VPN ページを開きます。

ステップ 6 この問題を報告している VPN 設定を選択します。

ステップ 7 [アクション] ペインで、[編集] アイコンをクリックします。

ステップ 8 各手順で [次へ] をクリックして、最後に手順 4 で [完了（Fnish）] ボタンをクリックします。

ステップ 9 すべてのデバイスの構成変更のプレビューと展開 （178 ページ）。

管理対象外 VPN ピアの導入準備

ピアの 1 つが導入準備されると、CDO はサイト間 VPN トンネルを検出します。2 番目のピアが CDO によって管理されていない場合は、VPN トンネルのリストをフィルタリングして、管理されていないデバイスを見つけて導入準備することができます。

ステップ 1 メインナビゲーションバーで、**[VPN]** > **[サイト間VPN]**を選択して VPN ページを開きます。

ステップ 2 [テーブルビュー（Table View）] を選択します。

ステップ 3 をクリックしてフィルタパネルを開きます。

ステップ 4 [管理対象外（Unmanaged）] にチェックを入れます。

ステップ 5 結果から管理対象外のデバイスを選択します。

ステップ 6 右側の [ピア（Peers）] ペインで、[デバイスの導入準備（Onboard Device）] をクリックし、画面の指示に従います。

関連情報：

- デバイスとサービスの導入準備
- ASA デバイスの導入準備

サイト間 VPN トンネルの検索とフィルタ処理

フィルタサイドバー を検索フィールドと組み合わせて使用して、VPN トンネル図に示されている VPN トンネルの検索を絞り込みます。

ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN] に進みます。

ステップ 2 フィルタアイコン をクリックしてフィルタペインを開きます。

ステップ 3 これらのフィルタを使用して検索を絞り込みます。

- [デバイスによるフィルタ] : [デバイスによるフィルタ] をクリックし、[デバイスタイプ] タブを選択し、フィルタ処理によって検索するデバイスをオンにします。
- [デバイスの問題] : トンネルの各サイドでの問題検出の有無。問題のあるデバイスの例としては、関連するインターフェイス、ピア IP アドレス、またはアクセスリストの欠落、IKEv1 プロポーザルの不一致などがありますが、これらに限定されません（トンネルの問題の検出は、AWS VPC VPN トンネルではまだ使用できません）。
- [デバイス/サービス] : デバイスのタイプ別にフィルタ処理します。
- [ステータス] : トンネルのステータスは、アクティブまたはアイドルになります。
  - [アクティブ] : セッションが開かれ、ネットワークパケットが VPN トンネルを通過している、または正常なセッションが確立され、タイムアウトになっていない場合。アクティブであることは、トンネルがアクティブで関連していることを示します。
  - [アイドル] : CDO が該当のトンネル用のセッションが開かれていることを検出できない、トンネルが使用されていない、またはトンネルに問題がある場合。
- [導入準備済み] : デバイスは、CDO によって管理される場合と、CDO によって管理されない場合（管理対象外）があります。
- [デバイスタイプ] : トンネルの各サイドが実際のデバイス（接続されたデバイス）かモデルデバイスか。

ステップ 4 検索バーにデバイス名または IP アドレスを入力して、フィルタ処理された結果を検索することもできます。検索では大文字と小文字は区別されません。

サイト間 VPN トンネルの IKE オブジェクトの詳細の表示

選択したトンネルのピア/デバイスで設定されている IKE オブジェクトの詳細を表示できます。それらの詳細は、IKE ポリシーオブジェクトの優先順位に基づいた階層のツリー構造に表示されます。

（注） エクストラネットデバイスには、IKE オブジェクトの詳細が表示されません。

ステップ 1 左側の CDO ナビゲーションバーで、[VPN] > [サイト間VPN] をクリックします。
ステップ 2 [VPNトンネル（VPN Tunnels）] ページで、ピアを接続する VPN トンネルの名前をクリックします。
ステップ 3 右側の [関係] で、詳細を表示するオブジェクトを展開します。

サイト間 VPN トンネルが最後に正常に確立された日を表示する

ステップ 1 サイト間 VPN トンネル情報の表示。
ステップ 2 [トンネルの詳細] ペインをクリックします。
ステップ 3 [最終アクティブ確認日（Last Seen Active）] フィールドを表示します。

サイト間 VPN トンネル情報の表示

サイト間 VPN テーブルビューは、CDO に導入準備されたすべてのデバイスで使用可能なすべてのサイト間 VPN トンネルの完全なリストです。トンネルは、このリストに 1 つだけ存在します。表にリストされているトンネルをクリックすると、右側のサイドバーにオプションが表示され、トンネルのピアに直接移動して詳細に調査できます。

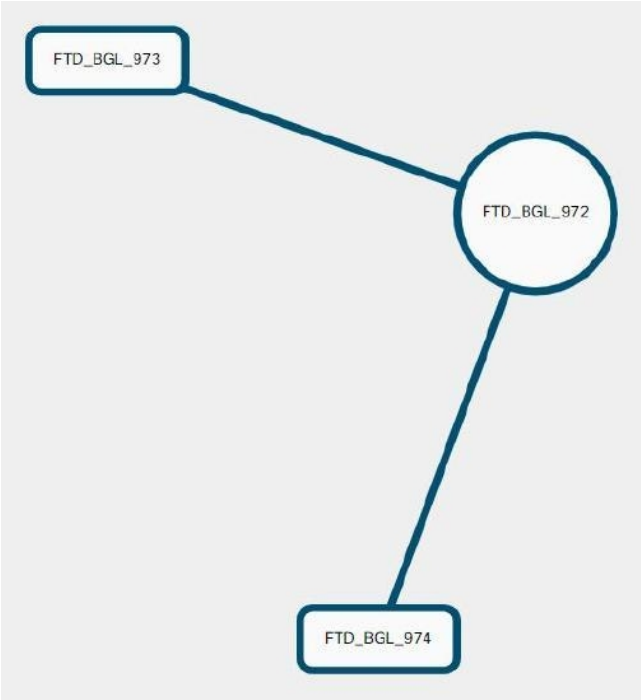
CDO がトンネルの両側を管理していない場合は、[導入準備デバイス（Onboard Device）] をクリックして、管理対象外のピアを導入準備するメインの導入準備ページを開くことができます。管理対象外 VPN ピアの導入準備 （76 ページ）CDO がトンネルの両側を管理する場合、[ピア2（Peer 2）] 列には管理対象デバイスの名前が含まれます。ただし、AWS VPC の場合、[ピア2（Peer 2）] 列には VPN ゲートウェイの IP アドレスが含まれています。

テーブルビューでサイト間 VPN 接続を表示するには、次の手順を実行します。

ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN] をクリックします。
ステップ 2 [テーブルビュー] ボタンをクリックします。
ステップ 3 「サイト間 VPN トンネルの検索とフィルタ処理」を使用して特定のトンネルを見つけるか、グローバルビューのグラフィックを拡大して、探している VPN ゲートウェイとそのピアを見つけます。

サイト間 *VPN* のグローバル表示

これは、グローバルビューの例です。この図では、「FTD_BGL_972」に FTD_BGL_973 デバイスおよび FTD_BGL_974 デバイスとのサイト間接続があります。



ステップ 1 メインのナビゲーションバーで、[VPN] > [サイト間VPN] をクリックします。

ステップ 2 [グローバルビュー（Global view）] ボタンをクリックします。

ステップ 3 「サイト間 VPN トンネルの検索とフィルタ処理」を使用して特定のトンネルを見つけるか、グローバルビューのグラフィックを拡大して、探している VPN ゲートウェイとそのピアを見つけます。

ステップ 4 グローバルビューに表示されているピアのいずれかを選択します。

ステップ 5 **[詳細の表示（View Details）]** をクリックします。

ステップ 6 VPN トンネルのもう一方の端をクリックすると、CDO は、その接続のトンネルの詳細、NAT 情報、およびキー交換情報を表示します。

- [トンネルの詳細]：トンネルの名前と接続情報が表示されます。[更新]アイコンをクリックすると、トンネルの接続情報が更新されます。
- [AWS接続固有のトンネルの詳細（Tunnel Details specific to AWS connections）]：AWS サイト間接続のトンネルの詳細は、他の接続の場合と若干異なります。AWS VPC から VPN ゲートウェイへの接続ごとに、AWS は 2 つの VPN トンネルを作成します。これは、ハイアベイラビリティを実現するためです。
  - トンネルの名前は、VPN ゲートウェイが接続されている VPC の名前を表します。トンネルの名前に含まれている IP アドレスは、VPN ゲートウェイが VPC として認識している IP アドレスです。

- CDO 接続の状態が「active」の場合、AWS トンネルの状態は「Up」です。CDO 接続の状態が「inactive」の場合、AWS トンネルの状態は「Down」です。

- [NAT情報（NAT Information）]：使用されている NAT ルールのタイプ、元のパケットの情報、および変換されたパケットの情報が表示され、そのトンネルの NAT ルールを確認できる NAT テーブルへのリンクが提供されます（AWS VPC サイト間 VPN ではまだ利用できません）。
- [キー交換]：トンネルで使用されている暗号キーと、キー交換の問題が表示されます（AWS VPC サイト間 VPN ではまだ利用できません）。

トンネルペイン

[トンネル（Tunnels）] ペインには、特定の VPN ゲートウェイに関連付けられているすべてのトンネルのリストが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続の場合、[トンネル（Tunnels）] ペインには、VPN ゲートウェイから VPC へのすべてのトンネルが表示されます。VPN ゲートウェイと AWS VPC のサイト間 VPN 接続にはそれぞれ 2 つのトンネルがあるため、他のデバイスで通常表示される 2 倍の数のトンネルが表示されます。

VPN ゲートウェイの詳細

VPN ゲートウェイに接続されているピア数と、VPN ゲートウェイの IP アドレスが表示されます。これは、[VPNトンネル（VPN Tunnels）] ページにのみ表示されます。

[ピア（Peers）] ペイン

サイト間 VPN ピアのペアを選択すると、ペアリングされた 2 つのデバイスのリストが [ピア（Peers）] ペインに表示され、いずれかのデバイスで [ピアの表示] をクリックできます。[ピアの表示（View Peers] をクリックすると、そのデバイスが関連付けられている他のサイト間ピアが表示されます。これは、テーブルビューとグローバルビューに表示されます。

リモートアクセス仮想プライベートネットワーク

リモートアクセス仮想プライベートネットワーク（RA VPN）では、各ユーザーがインターネットに接続されたコンピュータまたはその他のサポート対象の iOS または Android デバイスを使用して、離れた場所からネットワークに接続できます。これにより、モバイルワーカーが各自のホームネットワークや公共のWi-Fiネットワークから接続できるようになります。

RA VPN 設定は、次のコンポーネントで構成されています。

- 接続プロファイル：リモートアクセス VPN 接続プロファイルを作成すると、ホームネットワークなどの外部ネットワークからでも、ユーザーは内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。接続プロファイルは、アイデンティティソースとグループポリシーで構成されます。

関連情報：

• ASA のリモートアクセス VPN を設定する （88 ページ）

リモートアクセス仮想プライベート ネットワーク セッションの監視

リモートアクセス仮想プライベートネットワーク（RA VPN）は、モバイルユーザーや在宅勤務者などのリモートユーザーにセキュアな接続を提供します。これらの接続をモニタリングすることで、接続とユーザーセッションのパフォーマンスの重要なインジケータを一目で把握できます。CDO リモートアクセス VPNのモニタリング機能を使用すると、リモートアクセス VPNの問題が存在するかどうか、および存在する場所を迅速に特定できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。また、必要に応じてリモートアクセス VPN ユーザーをログアウトできます。

[リモートアクセス仮想プライベートモニタリング（Remote Access Virtual Private Monitoring）] ページには、[ライブ] と [履歴] の 2 つのビューがあります。テナント内のすべての 適応型セキュリティアプライアンス（ASA） VPN ヘッドエンドの AnyConnect リモートアクセス VPN セッションからリアルタイムデータまたは履歴データをモニタリングするために必要なビューを選択できます。

[リモートアクセス仮想プライベートモニタリング（Remote Access Virtual Private Monitoring）] ページには、各 RA VPN セッションからの次の情報が表示されます。

- RA VPN セッションからのライブデータと履歴データを提供します。
- CDO が管理するすべてのアクティブな VPN ヘッドエンドから一目でわかるビューを提供する直感的なグラフィカルビジュアルを表示します。
- ライブセッション画面には、CDO テナントで最も使用されているオペレーティングシステムと VPN 接続プロファイルが表示されます。また、平均セッション時間とアップロードおよびダウンロードされたデータも表示されます。
- ライブセッション画面には、RA VPN ヘッドエンドに接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。
- 履歴セッション画面には、過去 24 時間、7 日間、および 30 日間にすべてのデバイスについて記録されたデータを示す棒グラフがプロットされます。
- デバイスの種類、セッションの長さ、アップロードとダウンロードのデータ範囲などの基準に基づいて検索を絞り込むための新しいフィルタリング機能を提供します。
- ユーザー名、ログイン時間、期間、およびセッションが非アクティブだった時間。
- エンタープライズ ネットワーク内で割り当てられた IP アドレスと、セッションが開始されたパブリック IP アドレス。
- セッションに関連付けられた接続プロファイルとグループポリシー情報。
- ユーザーセッションで使用される AnyConnect のバージョンとオペレーティングシステムのタイプ。
- セッションタイムアウトまでの残りのアイドル時間。

関連情報：

- AnyConnect リモートアクセス VPN ライブセッションのモニタリング （82 ページ）
- AnyConnect リモートアクセス VPN セッション履歴のモニターリング （84 ページ）
- リモートアクセス VPN セッションの検索とフィルタ処理
- リモートアクセス VPN モニタリングビューのカスタマイズ
- RA VPN セッションの CSV ファイルへのエクスポート
- ユーザーのすべてのアクティブな RA VPN セッションの切断

AnyConnect リモートアクセス VPN ライブセッションのモニタリング

デバイス上のアクティブな AnyConnect RA VPN セッションからのリアルタイムデータを監視できます。このデータは 10 分ごとに更新されます。画面の右隅に表示されるリロードアイコン をクリックすると、最新のデータを確認できます。

始める前に

- RA VPN ヘッドエンドを CDO に導入準備します。
- ライブデータを監視するデバイスの接続ステータスは、[インベントリ] ページで「オンライン」になっています。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN] > [リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

または、CDO ホームページで [アクティブリモートアクセスVPNセッションの表示（View Active Remote Access VPN Sessions）] をクリックするか、**[VPN] > [リモートアクセスVPN（Remote Access VPN）]** に移動して、右上隅の アイコンをクリックします。

ステップ 2 [ライブ] をクリックします。

CDO はデバイスからのライブ情報の取得を開始し、[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）] ビューに RA VPN セッションを表示します。

（注） CDO がデバイスから情報を取得しないようにする場合は、[キャンセル] をクリックします。

ライブデータの表示

ライブデータは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [チャートビューの表示（Show Charts View）] アイコンをクリックする必要があります。

ダッシュボードには、CDO によって管理されるすべてのアクティブな VPN ヘッドエンドからの一目でわかるビューが表示されます。

- [内訳（すべてのデバイス）（Breakdown (All Devices)）]：ライブセッションの合計数が表示されます。また、4 つの弧の長さに分割された円グラフも表示されます。これは、セッション数が最も多い上位 3 つのデバイスの VPN セッションの割合を示しています。残りの弧の長さは、他のデバイスの総計を表します。
- CDO テナントで最も使用されているオペレーティングシステムと接続プロファイルが表示されます。
- 平均セッション時間とアップロードおよびダウンロードされたデータが表示されます。
- [国別のアクティブセッション（Active Sessions by Country）]：RA VPN ヘッドエンドに接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。
  - ユーザーセッションがある国は、青の色合いで表示されます。
  - マップの下部にある凡例は、国のセッション数とその国の色に使用される青の色合いとの相関関係を示すスケールが表示されます。
  - 地図上にマウスポインタを合わせると、国名とアクティブなユーザーセッションの総数が表示されます。
  - テーブルにマウスポインタを合わせると、その国の場所とアクティブなユーザーセッションの総数が地図上に表示されます。

表形式のビュー

表形式のビューのみを表示するには、画面の右上隅に表示される [表形式のビューを表示（Show Tabular View）] アイコンをクリックする必要があります。

表形式のビューには、現在接続している VPN ユーザーの完全なリストが表示されます。

- [場所（Location）] 列には、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユーザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 CDOは、ライブデータに標準フィルタを適用し、ダッシュボードにデータを表示します。ダッシュボードではカスタムフィルタはサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。新たに適用されたフィルタをクリアすると、ダッシュボードが再起動します（画面で[クリア]をクリックして、適用されたフィルタを手動で削除します）。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）]機能を使用して、デバイスタイプ、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの基準に基づいて検索を絞り込むことができます。リモートアクセス VPN セッションの検索とフィルタ処理 （85 ページ）一度に表示できる結果は最大 10,000 件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブなVPNユーザーのセッションを示します。

AnyConnect リモートアクセス VPN セッション履歴のモニターリング

過去 3 ヵ月間に記録された AnyConnect リモートアクセス VPN セッションの履歴データをモニターリングできます。

始める前に

- RA VPN ヘッドエンドの CDO への導入準備をします。
- 履歴データを監視するデバイスの接続状態は、[インベントリ] ページで「オンライン」になっています。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN] > [リモートアクセスVPNのモニターリング（Remote Access VPN Monitoring）]** をクリックします。

または、CDO ホームページで [アクティブリモートアクセスVPNセッションの表示（View Active Remote Access VPN Sessions）] をクリックするか、**[VPN] > [リモートアクセスVPN（Remote Access VPN）]**に移動して、右上隅の アイコンをクリックします。

ステップ 2 [履歴] をクリックします。

CDO には、過去 3 ヵ月間に記録された RA VPN セッションの履歴データが表示されます。

（注） CDOがデバイスから情報を取得しないようにする場合は、[キャンセル]（Cancel）]をクリックします。

履歴データの表示

履歴データは、ダッシュボードと表形式の両方で表示されます。

[ダッシュボード（Dashboard）] ビュー

ダッシュボードを表示するには、画面の右上隅に表示される [チャートビューの表示（Show Charts View）] アイコンをクリックする必要があります。表形式のビューとともに、ダッシュボードビューが表示されます。

ダッシュボードには、CDO によって管理されるすべてのアクティブな VPN ヘッドエンドからの一目でわかるビューが表示されます。過去 24 時間、7 日間、および 30 日間にすべてのデバイスで記録された VPN セッションを示す棒グラフが表示されます。ドロップダウンから期間を選択できます。個々のバーにカーソルを合わせると、日付とその日の合計セッション数が表示されます。

表形式のビュー

表形式のビューのみを表示するには、画面の右上隅に表示される [表形式のビューを表示（Show Tabular View）] アイコンをクリックする必要があります。表形式には、過去 3 ヵ月間に接続した VPN ユーザーの完全なリストが表示されます。

[場所（Location）] カラムには、パブリック IP アドレスを地理的に配置することにより、VPN ヘッドエンドに接続されているすべてのユーザーの場所が表示されます。行をクリックして、ユーザーの詳細を表示します。左ペインのロケーションリンクをクリックすると、ユーザーの場所が Google マップ上に表示されます。

重要 CDO は、履歴データに標準フィルタを適用し、ダッシュボードに表示します。ダッシュボードではカスタムフィルタはサポートされていないため、表形式のデータが表示されている場合にのみ、新しいフィルタを適用できます。新たに適用されたフィルタをクリアすると、ダッシュボードが再起動します（画面で [クリア] をクリックして、適用されたフィルタを手動で削除します）。標準フィルタは削除できません。

[RA VPNセッションの検索およびフィルタリング（Search and Filter RA VPN Sessions）]リモートアクセス VPN セッションの検索とフィルタ処理（85 ページ）機能を使用して、セッションの日と時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいて検索を絞り込むことができます。一度に表示できる結果は最大 10,000 件です。

ステータス列の「アクティブ（Active）」ラベルの付いた緑色の点は、アクティブな VPN ユーザーのセッションを示します。

リモートアクセス VPN セッションの検索とフィルタ処理

検索（Search）

検索バー機能を使用して、RA VPN セッションを検索します。検索バーにデバイス名、IP アドレス、またはシリアル番号を入力し始めると、検索条件に一致する RA VPN セッションが表示されます。検索では大文字と小文字が区別されません。

Filter

フィルタサイドバーを使用して、セッション時間の範囲、セッションの長さ、アップロードおよびダウンロードのデータ範囲などの条件に基づいてRA VPNを特定できます。フィルタ機能は、ライブビューと履歴ビューの両方で使用できます。

- [デバイス]：1 つまたはすべてのデバイスを選択して、選択したデバイスからのセッションを表示します。
- [セッションの時間範囲（Sessions Time Range）]（履歴データにのみ適用）：指定した日時範囲のセッションの履歴を表示します。表示できるのは、過去 3 ヵ月間に記録されたデータのみです。
- [セッションの長さ（Sessions Length）]：指定されたセッションの継続時間に基づいてセッションを表示します。時間の単位（時間、分、または秒）を設定し、スライダを動かして、継続時間の最小長と最大長を指定します。表示されたフィールドで長さを指定することもできます。
- [アップロード（TX）（Upload (TX)）]：セキュリティで保護されたネットワークにアップロードまたは転送されたデータの指定量に基づいてセッションを表示します。単位（GB、MB、またはKB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。
- [ダウンロード（RX）（Download (RX)）]：セキュリティで保護されたネットワークからダウンロードまたは受信したデータの指定量に基づいてセッションを表示します。単位（GB、MB、または KB）を設定し、スライダを適宜動かして範囲を選択します。表示されるフィールドに値を指定することもできます。

リモートアクセス VPN モニタリングビューのカスタマイズ

ライブモードと履歴モードの両方のリモートアクセス VPN モニタリングビューを変更して、必要なビューに適用される列ヘッダーのみを含めることができます。列の右側にある列フィルタアイコン  をクリックし、必要な列を選択または選択解除します。

CDO に次回サインインしたとき、選択した内容が CDO に記憶されています。

RA VPN セッションの CSV ファイルへのエクスポート

1 つ以上のデバイスの RA VPN セッションをコンマ区切り値（.csv）ファイルにエクスポートできます。Microsoft Excel などのスプレッドシート アプリケーションで .csv ファイルを開いて、リストの項目を並べ替えたり、フィルタ処理したりできます。この情報は、RA VPN セッションの分析に役立ちます。セッションをエクスポートするたびに、CDO は new.csv ファイルを作成します。作成されるファイルの名前には日付と時刻が含まれます。

CDO は、最大 100,000 のアクティブセッションを CSV ファイルにエクスポートできます。すべてのデバイスからのセッションの合計数が上限を超えている場合は、[デバイス別表示（View By Device）] フィルタを使用して、個々のデバイスのレポートを生成できます。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニタリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 [デバイス別表示（View By Devices）] 領域で、次のいずれかを選択します。

- [すべてのデバイス（All Devices）] は、その下に一覧表示されているすべてのデバイスからアクティブセッションをエクスポートします。
- セッションをエクスポートするデバイスをクリックします。

ステップ 3 右上隅の アイコンをクリックします。CDO は、画面に表示されているルールを .csv ファイルにエクスポートします。

ステップ 4 スプレッドシートアプリケーションで .csv ファイルを開いて、結果を並べ替えたりフィルタリングしたりすることができます。

ASA ユーザーのアクティブな RA VPN セッションの切断

ASA デバイス上のすべてのユーザーのアクティブな RA VPN セッションを終了できます。このタスクは、ライブモードと履歴モードの両方で実行できます。

CDO は、ユーザーが VPN セッションを表示および終了できるようにする VPN セッション マネージャー ユーザー ロールを提供します。詳細については、「ユーザーロール」を参照してください。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニターリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 [デバイス別表示（View By Devices）] 領域で、デバイス上のすべてのアクティブなセッションを終了する ASA デバイスをクリックします。

ステップ 3 右上隅に表示される [すべてのセッションを終了（Terminate All Sessions）] をクリックします。

ステップ 4 [はい、すべてのセッションを終了します（Terminate All Sessions）] をクリックして、選択を確定します。

ユーザーのすべてのアクティブな *RA VPN* セッションの切断

CDO は、ユーザーを接続解除すると、ASA デバイス上のユーザーのアクティブな RA VPN セッションをすべて終了します。このタスクは、ライブモードと履歴モードの両方で実行できます。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNのモニターリング（Remote Access VPN Monitoring）]** をクリックします。

ステップ 2 セッションを切断するユーザーを検索します。[検索（Search）] バーに、検索条件を入力できます。

ステップ 3 アクティブなセッションをクリックし、右側の [アクション] ペインで、[このユーザーのすべてのRA VPN セッションを終了する（Terminate all RA VPN sessions for this user）] リンクをクリックします。

ASA のリモートアクセス VPN を設定する

ASACisco Secure Firewall Cloud Native は、ユーザーがプライベート接続と見なす TCP/IP ネットワーク（インターネットなど）全体でセキュアな接続を確立することにより、仮想プライベートネットワークを構築します。これによって、single-user-to-LAN 接続と LAN-to-LAN 接続を確立できます。

セキュアな接続はトンネルと呼ばれ、ASA はトンネリング プロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを介したパケットの送受信、パケットのカプセル化解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。

CDO は、新しいリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するための直感的なユーザーインターフェイスを提供します。また、CDO に導入準備された複数の適応型セキュリティアプライアンス（ASA）デバイスの RA VPN 接続をすばやく簡単に設定できます。

CDO を使用して、ASA デバイスで RA VPN 構成をゼロから設定できます。また、Adaptive Security Defense Manager（ASDM）や Cisco Security Manager（CSM）などの他の ASA 管理ツールを使用して構成済みの RA VPN 設定を管理することもできます。RA VPN 設定がすでにある ASA デバイスを導入準備すると、CDO は自動的に「デフォルトの RA VPN 構成」を作成し、ASA デバイスをこの構成に関連付けます。このデフォルト構成には、デバイスで定義されているすべての接続プロファイルオブジェクトを含めることができます。CDO に読み取られる RA VPN 属性を理解するには、「オンボーディング済み ASA デバイスの RA VPN 設定の読み取り」セクションを参照してください。それ以外の場合は、「ASA のエンドツーエンド リモート アクセス VPN 構成プロセス」で説明されている手順を実行してください。

関連情報：

- ASA のエンドツーエンド リモート アクセス VPN 設定プロセス
  - ASA のアイデンティティ ソースを設定する
    - ASA Active Directory レルム オブジェクトの作成または編集
    - ASA RADIUS サーバーオブジェクトまたはグループの作成または編集
  - 新規 ASA RA VPN グループポリシーの作成 （96 ページ）
  - ASA RA VPN 設定の作成 （105 ページ）
  - ASA RA VPN 接続プロファイルの設定 （109 ページ）

- オンボーディング済み ASA デバイスの RA VPN 設定の読み取り
- IP アドレスプールの作成
- NAT からの ASA リモート アクセス トラフィックの除外 （127 ページ）
- ASA のリモートアクセス VPN 設定の確認
- ASA のリモートアクセス VPN 設定の詳細表示

ASA のエンドツーエンド リモート アクセス VPN 設定プロセス

このセクションでは、CDO に導入準備された ASA デバイスでリモートアクセス仮想プライベートネットワーク（RA VPN）を設定するためのエンドツーエンドの手順について説明します。

クライアントのリモートアクセス VPN を有効化するには、いくつかの異なる項目を設定する必要があります。次の手順では、エンドツーエンドのプロセスについて説明します。

ステップ 1 リモート ユーザを認証する目的で使用されるアイデンティティ ソースを設定します。詳細については、「ASA のアイデンティティソースを設定する」を参照してください。

次のソースを使用して、RA VPN を使用してネットワークに接続しようとするユーザーを認証できます。さらに、クライアント証明書を単独で、またはアイデンティティソースと連携させて、認証に使用できます。

- Active Directory アイデンティティレルム：プライマリ認証ソースとして使用できます。ユーザ アカウントは Active Directory（AD）サーバで定義されます。「AD アイデンティティレルムの設定」を参照してください。「ASA Active Directory レルム オブジェクトの作成または編集」を参照してください。
- RADIUS サーバーグループ：プライマリまたはセカンダリ認証ソースとして使用でき、認可およびアカウンティングに使用できます。「ASA RADIUS サーバーオブジェクトまたはグループの作成または編集」を参照してください。
- ローカル ID ソース（ローカルユーザーデータベース）：プライマリソースまたはフォールバックソースとして使用できます。デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。フォールバックソースとしてローカルデータベースを使用する場合は、必ず外部サーバーで定義したものと同じユーザー名/パスワードを定義します。注：ASA デバイスで直接ユーザーアカウントを作成できるのは、Adaptive Security Device Manager（ASDM）からのみです。『Cisco ASA Series Firewall ASDM Configuration Guide, XY』の「Objects for Access Control」の章の「Configure Local User Groups」セクションを参照してください

ステップ 2 （任意）新規 ASA RA VPN グループポリシーの作成 （96 ページ）。グループポリシーは、ユーザーに関連する属性を定義します。グループメンバーシップに基づいて、リソースへの差分アクセスを提供するためにグループポリシーを設定することができます。または、すべての接続でデフォルトポリシーを使用します。

ステップ 3 ASA RA VPN 設定の作成 （105 ページ）。

ステップ 4 ASA RA VPN 接続プロファイルの設定 （109 ページ）。

ステップ 5 （任意）NAT からの ASA リモート アクセス トラフィックの除外 （127 ページ）。

ステップ 6 CDO から ASA に設定変更を展開します。。

重要 Adaptive Security Device Manager（ASDM）などのローカルマネージャーを使用してリモートアクセス VPN の設定を変更すると、CDO では、そのデバイスの [設定ステータス（Configuration Status）] に [競合検出（Conflict Detected）] と表示されます。「デバイスのアウトオブバンド変更」を参照してください。この ASA で設定の競合の解決できます。

次のタスク

次の手順

RA VPN 設定が ASA デバイスにダウンロードされると、ユーザーは、インターネットに接続されているコンピュータやその他のサポートされている iOS または Android デバイスを使用して、リモートの場所からネットワークに接続できます。テナント内のすべての導入準備 ASA RA VPN ヘッドエンドから、ライブ AnyConnect リモートアクセス仮想プライベートネットワーク（RA VPN）セッションを監視できます。「リモートアクセス仮想プライベート ネットワーク セッションの監視」を参照してください。

ASA のアイデンティティ ソースを設定する

Microsoft Active Directory（AD）レルムや RADIUS サーバーなどのアイデンティティ ソースは、組織内のユーザーのユーザーアカウントを定義する AAA サーバーおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、CDO へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

[オブジェクト] > [オブジェクトの作成]（  ）> [アイデンティティ ソース] をクリックしてソースを作成します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。適切なフィルタを適用して既存のソースを検索し、それらを管理できます。

ディレクトリ ベースの DN の決定

ディレクトリの各プロパティを設定する際、ユーザおよびグループに共通のベース識別名（DN）を指定する必要があります。ベースはディレクトリサーバー内で定義され、ネットワークごとに異なります。アイデンティティ ポリシーが正しく機能するには、適切なベースを入力する必要があります。ベースが誤っていると、ユーザ名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。

（注） 正しいベースを取得するには、ディレクトリ サーバを担当する管理者に確認してください。

Active Directory の場合、ドメイン管理者として Active Directory サーバーにログインし、コマンドプロンプトで **dsquery** のコマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べたい既知のユーザー名（一部または全体）を指定します。たとえば、次のコマンドでは、「John*」という部分名を使用して、「John」から始まるすべてのユーザーの情報を返します。

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

dsquery group コマンドを入力し、ベース識別名を調べたい既知のグループ名（一部または全部）を指定します。たとえば、次のコマンドは、Employees グループ名を使用して次に識別名を返します。

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

グループのベース DN は、「DC=csc-lab,DC=example,DC=com」となります。

ADSI Edit プログラムを使用して、Active Directory 構造を参照することもできます（**[スタート（Start）] > [ファイル名を指定して実行（Run）] > [adsiedit.msc]**）。ADSI Edit で組織ユニット（OU）、グループ、ユーザーなどのオブジェクトを右クリックし、[プロパティ（Properties）] を選択すると、識別名が表示されます。DC 値の文字列を、ベースとしてコピーします。

正しいベースであることを確認するには、次の手順を実行します。

ステップ 1 ディレクトリ プロパティの [テスト接続（Test Connection）] ボタンをクリックし、接続を確認します。問題があった場合には修正して、ディレクトリ プロパティを保存します。

ステップ 2 変更をデバイスに適用します。

ステップ 3 アクセス ルールを作成して、[ユーザ（Users）] タブを選択し、ディレクトリから既知のユーザおよびグループ名の追加を試みます。ディレクトリを含むレルム内の一致ユーザ名およびグループ名を入力すると、入力中にオートコンプリートによる候補が表示されます。ドロップダウン リストに候補が表示される場合は、システムがディレクトリに適切に照会できたことを意味します。入力した文字列がユーザ名またはグループ名として表示されることが確かであるにもかかわらず、候補が表示されない場合は、対応する検索ベースを修正する必要があります。

次のタスク

詳細については、「ASA Active Directory レルム オブジェクトの作成または編集」を参照してください。

RADIUS サーバおよびグループ

RADIUS サーバーを使用して、管理ユーザーを認証および認可できます。RADIUS サーバを使用するように機能を設定する場合は、個別のサーバではなく RADIUS グループを選択します。RADIUS グループは、相互にコピーである RADIUS サーバの集合です。グループに複数のサー

バがある場合は、それらは、1 つのサーバが使用できなくなった場合に冗長性を提供する一連のバックアップサーバを形成します。ただし、サーバが1つしかない場合でも、機能のRADIUSサポートを設定するには、メンバーが 1 つのグループを作成する必要があります。

このソースは、以下の目的で使用できます。

- 認証、および許可、アカウンティングのアイデンティティソースとしてのリモートアクセス VPN。AD は RADIUS サーバーと組み合わせて使用できます。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザー アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

詳細については、「ASA RADIUS サーバーオブジェクトまたはグループの作成または編集」を参照してください。

ASA Active Directory レルム オブジェクトの作成または編集

AD レルムオブジェクトなどの ID ソースオブジェクトを作成または編集すると、CDO は SDC を介して ASA デバイスに設定要求を送信します。次に ASA は、設定された AD レルムと通信します。

次の手順を使用して、オブジェクトを作成します。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 **[オブジェクトの作成]**（  ）**[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [アイデンティティ ソース（Identity Source 0]**をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object Name）] を入力します。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 ウィザードの最初の部分で、[IDソースタイプ（Identity Source Type）]として [Active Directoryレルム（Active Directory Realm）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 基本レルムのプロパティを設定します。

- [ディレクトリユーザー名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザー情報に対して適切な権限を持つユーザーの識別用ユーザー名とパスワード。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザー名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

  （注） この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザーは、共通名の「users」フォルダの下で設定する必要があります。

- [ベース識別名（Base Distinguished Name）]：ユーザーおよびグループ情報、つまり、ユーザーとグループの共通の親を検索またはクエリするためのディレクトリツリー。例、cn=users,dc=example,dc=com。

ステップ 7 ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリ サーバのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化（Encryption）]：ユーザーおよびグループ情報のダウンロードに暗号化接続を使用するには、[LDAPS] を選択し、SSL を使用して ASA と LDAP サーバー間の通信を保護します。LDAP over SSL が必要です。ポート 636 を使用します。

  デフォルトでは[なし（None）]になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。

ステップ 8 （オプション）[テスト（Test）] ボタンを使用して、構成を検証します。

ステップ 9 （オプション）[別の構成を追加（Add another configuration）] をクリックして、複数の Active Directory（AD）サーバーを AD レルムに追加します。AD サーバーは互いの複製である必要があり、同じ AD ドメインをサポートする必要があります。したがって、ディレクトリ名、ディレクトリパスワード、ベース識別名などの基本的なレルムプロパティは、その AD レルムに関連付けられたすべての AD サーバーで同じ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。

ASA Active Directory レルム オブジェクトの編集

アイデンティティ ソース オブジェクトの編集時にアイデンティティ ソース タイプを変更できないことに注意してください。正しいタイプの新しいオブジェクトを作成する必要があります。

ステップ 1 ナビゲーションバーで、[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 編集するオブジェクトを選択します。

ステップ 4 詳細パネルの [操作（Actions）] ウィンドウにある編集アイコン  をクリックします。

ステップ 5 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。下に表示される設定バーを展開し、ホスト名/IP アドレスや暗号化情報を編集またはテストします。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 CDO は、変更の影響を受けるポリシーを表示します。[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ポリシーへの変更を確定します。

ステップ 8 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機してから複数の変更を一度に展開します。

ASA RADIUS サーバーオブジェクトまたはグループの作成または編集

RADIUS サーバーオブジェクトや RADIUS サーバーオブジェクトのグループなどの ID ソースオブジェクトを作成または編集すると、CDO は SDC を介して設定要求を ASA デバイスに送信します。

RADIUS サーバーオブジェクトの作成

RADIUS サーバーは、AAA（認証、認可、アカウンティング）サービスを提供します。

次の手順を使用して、オブジェクトを作成します。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 **[オブジェクトの作成]**（+）> **[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）]** > **[アイデンティティ ソース]**をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [アイデンティティ ソース タイプ（Identity Source Type）] として [RADIUSサーバーグループ（RADIUS Server Group）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 次のプロパティを使用して ID ソース設定を編集します。

- [サーバー名またはIPアドレス（Server Name or IP Address）]：サーバーの完全修飾ホスト名（FQDN）または IP アドレス。
- [認証ポート（Authentication Port）]（オプション）：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [タイムアウト（Timeout）]：次のサーバーに要求を送信する前にサーバーからの応答を待機する時間の長さ（1 ～ 300 秒）。デフォルトは 10 秒です。
- [サーバー秘密キー（Server Secret Key）] の入力（オプション）：ASA デバイスと RADIUS サーバー間でデータを暗号化するために使用される共有秘密。キーは、大文字と小文字が区別される最大 64 文字の英数字文字列です。スペースは使用できません。キーは、英数字または下線で開始する必要があります。特殊文字 $ & - _ . + @ を使用できます。文字列は、RADIUS サーバーで設定された文字列と一致している必要があります。秘密キーを設定していない場合、接続は暗号化されません。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機してから複数の変更を一度に展開します。

RADIUS サーバーグループの作成

RADIUS サーバーグループには、1 つまたは複数の RADIUS サーバーオブジェクトが含まれています。グループ内のサーバーは、相互にコピーされる必要があります。グループ内のサーバーでバックアップサーバーのチェーンが形成されるため、最初のサーバーが利用できなった場合、システムはリスト上の次のサーバーを試すことができます。

次の手順を使用して、オブジェクトグループを作成します。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] をクリックします。

ステップ 2 **[オブジェクトの作成]**（  ）**[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] [アイデンティティソース（Identity Source 0]** をクリックします。

ステップ 3 オブジェクトの [オブジェクト名（Object name）] を入力します。

ステップ 4 [デバイスタイプ（Device Tipe）] で [ASA] を選択します。

ステップ 5 [アイデンティティ ソース タイプ（Identity Source Type）] として [RADIUSサーバーグループ（RADIUS Server Group）] を選択します。[続行（Continue）] をクリックします。

ステップ 6 次のプロパティを使用して ID ソース設定を編集します。

- [デッドタイム（Dead Time）]：失敗したサーバーは、すべてのサーバーが失敗した後にのみ再アクティブ化されます。デッドタイムは、最後のサーバーが失敗した後にすべてのサーバーを再アクティブ化するまで待機する時間の長さです。
- [最大失敗試行回数（Maximum Failed Attempts）]：次のサーバーを試行する前に、グループ内の RADIUS サーバーに送信されて失敗した要求の数（応答がなかった要求の数）。最大失敗試行回数を超えると、システムはそのサーバーを故障としてマークします。特定の機能について、ローカルデータベースを使用するフォールバック方式を設定していて、グループ内のすべてのサーバーが応答に失敗した場合、そのグループは非応答と見なされ、フォールバック方式が試行されます。サーバーグループはデッドタイムの間、非応答とマークされたままになるため、その期間内に追加の AAA 要求でサーバーグループへの接続は試行されず、フォールバック方式がすぐに使用されます。
- （任意）[ダイナミック認証/ポート（Dynamic Authorization/Port）]：RADIUS サーバーグループ向けの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にすると、そのグループは CoA 通知用に登録され、Cisco Identity Services Engine（ISE）からの CoA ポリシー更新を指定したポートでリッスンします。このサーバー グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

ステップ 7 ドロップダウンメニューから、RADIUS サーバーをサポートする AD レルムを選択します。AD レルムをまだ作成していない場合は、ドロップダウンメニューの [作成（Create）] をクリックします。

ステップ 8 [RADIUSサーバーの追加（RADIUS SERVER Add）] ボタン  をクリックして、既存の RADIUS サーバーオブジェクトを追加します。必要に応じて、このウィンドウから新しい RADIUS サーバーオブジェクトを作成できます。

（注） リストの最初のサーバーは応答しなくなるまで使用されるため、作成したサーバーオブジェクトを優先して追加します。その後、ASA はデフォルトでリスト内の次のサーバーに設定されます。

ステップ 9 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機してから複数の変更を一度に展開します。

RADIUS サーバーオブジェクトまたはグループの編集

RADIUS サーバーオブジェクトまたは RADIUS サーバーグループを編集するには、次の手順を使用します。

ステップ 1 ナビゲーションバーで、[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（search）] 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 編集するオブジェクトを選択します。

ステップ 4 詳細パネルの [アクション] ペインにある [編集] アイコン をクリックします。

ステップ 5 前述の手順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。ホスト名/IP アドレスまたは暗号化情報を編集またはテストするには、設定バーを展開します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 CDO は、変更の影響を受けるポリシーを表示します。[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ポリシーへの変更を確定します。

ステップ 8 行った変更を今すぐCDO から ASA に設定変更を展開します。か、待機して、複数の変更を同時に展開します。

新規 *ASA RA VPN* グループポリシーの作成

グループポリシーは、リモートアクセス VPN ユーザーの一連のユーザー指向属性値ペアです。接続プロファイルでは、トンネル確立後、ユーザー接続の条件を設定するグループポリシーが使用されます。グループ ポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

システムには、「DfltGrpPolicy」という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

（注） 不整合のあるグループ ポリシー オブジェクトを RA VPN 設定に追加することはできません。グループポリシーを RA VPN 設定に追加する前に、すべての不整合を解決してください。

ステップ 1 ナビゲーションバーで、[オブジェクト（Objects）] 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ます。

ステップ 3 **[RA VPNオブジェクト（ASAおよびFTD）（RA VPN Objects (ASA & FTD)）] > [RA VPNグループポリシー（RA VPN Group Policy）]** をクリックします。

ステップ 4 グループ ポリシーの名前を入力します。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。

ステップ 5 [デバイスタイプ] ドロップダウンで、[ASA] を選択します。

ステップ 6 次のいずれかを実行します。

- 必要なタブをクリックし、そのページで属性を設定します。

ステップ 7 [保存（Save）] をクリックしてグループポリシーを作成します。

ASA RA VPN グループポリシー属性

このセクションでは、ASA RA VPN グループポリシーに関連付けられた属性について説明します。

一般属性

グループポリシーの全般的な属性では、グループの名前およびその他の基本設定を定義します。

- [DNSサーバー（DNS Server）]：VPN接続時にドメイン名を解決するためのDNSサーバーのIPアドレスを入力します。コンマを使用してアドレスを区切ることができます。
- **Banner**：ユーザーのログイン時に表示するバナーテキストまたはウェルカムメッセージです。デフォルトでは、バナーは表示されません。最大文字数は496文字です。AnyConnectクライアントは、部分的なHTMLをサポートしています。リモートユーザーへバナーが適切に表示されることを確認するには、
タグを使用して改行を示します。
- [デフォルトドメイン（Default Domain）]：RA VPN内のユーザーのデフォルトドメインの名前。例、example.com。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。

AnyConnect クライアント プロファイル

この機能は、ソフトウェアバージョン6.7以降のバージョンを実行しているFTDでサポートされています。

Cisco AnyConnect VPNクライアントは、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。

VPN ユーザーが VPN AnyConnect クライアントソフトウェアをダウンロードするときに、クライアントにダウンロードする AnyConnect VPN プロファイルオブジェクトと AnyConnect モジュールを選択できます。

1. AnyConnect VPN プロファイルオブジェクトを選択または作成します。「RA VPN AnyConnect クライアントプロファイルのアップロード （130 ページ）」を参照してください。DART および Start Before Login モジュールを除き、AnyConnect VPN プロファイルオブジェクトを選択する必要があります。

2. [AnyConnectクライアントモジュールの追加（Add Any Connect Client Module）] をクリックします。

   次の AnyConnect モジュールはオプションであり、VPN AnyConnect クライアントソフトウェアとともに各モジュールがダウンロードされるように設定できます。

   - **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**：システムログのスナップショットおよびその他の診断情報がキャプチャされて、.zip ファイルがデスクトップに作成されるため、トラブルシューティング情報を簡単に Cisco TAC に送信できます。
   - **フィードバック**：お客様が有効にして使用している機能とモジュールに関する情報を提供します。
   - **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。
   - **Network Access Manager**：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。
   - **Network Visibility**：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 AnyConnect を開始することにより、Windows にログインする前のユーザーを VPN 接続を介して企業インフラストラクチャに強制的に接続させます。
   - **Cisco 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。

3. [クライアントモジュール（Client Module）] リストで [AnyConnect] モジュールを選択します。

4. [プロファイル（Profile）] リストで、AnyConnect クライアントプロファイルを含むプロファイルオブジェクトを選択または作成します。

5. [モジュールのダウンロードを有効化（Enable Module Download）] をオンにすると、エンドポイントで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。

セッション設定属性

グループポリシーのセッションの設定は、VPN を通じて接続できる時間と、接続を確立できる個別の接続数を制御します。

- [最大接続時間（Maximum Connection Time）]：ユーザーがログアウト、再接続せずに VPN に接続したままにできる最大時間（分）で、1 ～ 4473924 または空白で指定します。デフォルトは無制限（空白）ですが、その場合でもアイドル タイムアウトは適用されます。
- [接続時間のアラート間隔（Connection Time Alert Interval）]：最大接続時間を指定した場合、アラート間隔は、次回の自動切断についてユーザーに警告を表示する最大時間に達するまでの時間を定義します。ユーザーは、接続を終了し、再接続してタイマーを再起動することを選択できます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [アイドルタイム（Idle Time）]：VPN 接続が自動的に閉じられる前にアイドル状態になる時間（分）で、1 ～ 35791394 で指定します。指定した時間、接続で通信アクティビティがない場合、システムは接続を停止します。デフォルトは 30 分です。
- [アイドル時間のアラート間隔（Idle Time Alert Interval）]：アイドルセッションが原因の次回の自動切断について、ユーザーに警告を表示するアイドル時間に達するまでの時間。アクティビティがあるとタイマーがリセットされます。デフォルトは 1 分です。1 ～ 30 分を指定できます。
- [ユーザーあたりの同時ログイン数（Simultaneous Login Per User）]：ユーザーに許可する同時接続の最大数。デフォルトは 3 です。1 ～ 2147483647 個の接続を指定できます。多数の同時接続を許可するとセキュリティの低下を招き、パフォーマンスに影響を及ぼす可能性があります。

アドレス割り当て属性

グループポリシーのアドレスの割り当て属性は、グループの IP アドレスプールを定義します。ここで定義されているプールで、このグループを使用するすべての接続プロファイルで定義済みのプールがオーバーライドされます。接続プロファイルで定義済みのプールを使用する場合は、これらの設定を空白のままにします。

- [IPv4アドレスプール]、[IPv6アドレスプール]：これらのオプションは、リモートエンドポイントのアドレスプールを定義します。クライアントには、VPN 接続のために使用する IP バージョンに基づき、これらのプールからアドレスが割り当てられます。サポートする IP タイプごとにサブネットを定義する IP アドレスプールを選択します。当該 IP バージョンをサポートしない場合は、リストを空のままにします。たとえば、IPv4 プールを「10.100.10.0/24」と定義できます。アドレス プールは、外部インターフェイスの IP アドレスと同じサブネット上に存在することはできません。新しい IP アドレスプールの作成を作成するには、次の手順を実行します。ローカルアドレスの割り当てに使用する最大 6 個のアドレスプールのリストを指定できます。プールの指定順序は重要です。システムで

は、プールの表示順に従いプールからアドレスが割り当てられます。**注**：同じグループポリシーで IPv4 と IPv6 両方のアドレスプールを設定できます。同じグループ ポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

- [DHCPスコープ]：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プール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 サーバーはアドレス 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。スコープを指定するには、ネットワーク番号のホストアドレスを含むネットワークオブジェクトを入力します。たとえば、192.168.5.0/24 サブネットプールのアドレスを使用するように DHCP サーバーに指示するには、ホストアドレスとして 192.168.5.0 を指定するネットワークオブジェクトを入力します。DHCP は IPv4 アドレス指定にのみ使用することができます。

スプリット トンネリング属性

グループポリシーのスプリットトンネリング属性は、システムが内部ネットワーク用のトラフィックと外部方向トラフィックを処理する方法を定義します。スプリットトンネリングは、VPN トンネル（暗号化）と VPN トンネル外の残りのネットワークトラフィック（非暗号化、つまりクリアテキスト）を介して一部のネットワークトラフィックを誘導します。

通常、リモートアクセス VPN では、VPN ユーザーに自社のデバイスを介してインターネットにアクセスさせます。ただし、RA VPN に接続している VPN ユーザーに、外部ネットワークへのアクセスを許可することができます。この技術は、スプリットトンネリングまたはヘアピニングと呼ばれます。スプリットトンネルでは、セキュアトンネル経由のリモートネットワークへの VPN 接続が可能ですが、VPN トンネル外のネットワークにも接続できます。スプリットトンネリングは、FTDデバイスのネットワーク負荷を軽減し、外部インターフェイスの帯域幅を拡大します。

はじめる前に

IPv4ネットワーク用とIPv6ネットワーク用のスプリットトンネルポリシーを作成する場合は、指定するアクセスリストが両方のプロトコルで使用されます。したがって、アクセスリストには、IPv4 トラフィックと IPv6 トラフィックの両方のアクセス コントロール エントリ（ACE）が含まれている必要があります。

ASA デバイスが CDO に導入準備されると、CDO はデバイスに関連付けられた拡張 ACL を読み取ります。詳細については、「Group Policy」を参照してください。新しい ACL を作成する場合は、「ASA ポリシー（拡張アクセスリスト）」を参照して作成してください。

（注） 作成する ACL の送信元ネットワークとして、スプリットトンネリング用のネットワークを指定していることを確認してください。

- [IPv4スプリットトンネリング（IPv4 Split Tunneling）]、[IPv6スプリットトンネリング（IPv6 Split Tunneling）]：トラフィックが IPv4 または IPv6 アドレスを使用するかどうかに基づいて、さまざまなオプションを指定できますが、それぞれのオプションは同じです。スプリットトンネリングを有効にする場合は、ネットワークオブジェクトを選択する必要があるいずれかのオプションを指定します。
  - [トンネル経由のトラフィックをすべて許可する（Allow all traffic over tunnel）]：スプリットトンネリングを行いません。ユーザーが RA VPN 接続を行うと、そのユーザーのトラフィックはすべて保護されたトンネルを通過します。これがデフォルトです。最も安全なオプションであるとも考えられます。
  - [トンネル経由の指定されたトラフィックを許可する（Allow specified traffic over the tunnel）]：送信元ネットワークを定義する拡張アクセスリストを選択します。これらの送信元からのトラフィックはすべて、保護されたトンネルを通過します。その他すべての送信元からのトラフィックは、クライアントによって、トンネル外の接続（ローカル Wi-Fi やネットワーク接続など）にルーティングされます。
  - [以下に指定したネットワークを除外する（Exclude networks specified below）]：送信元ネットワークを定義するネットワークオブジェクトを選択します。クライアントは、指定された送信元からのトラフィックをトンネル外の接続にルーティングします。他の送信元からのトラフィックはトンネルを通過します。
  - [ネットワークリスト（Network List）]：IPv4 と IPv6 ネットワークの両方を持つことができる拡張 ACL ネットワークを選択します。
- [スプリットDNS（Split DNS）]：クライアントが、そのクライアントで設定されている DNS サーバーに他の DNS 要求を送信することを許可しながら、セキュアな接続を介して一部の DNS 要求を送信するようにシステムを設定できます。次の DNS 動作を設定できます。
  - [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）]：このオプションを選択すると、スプリット トンネル オプションが定義されている場合と同じ方法で DNS 要求が処理されます。スプリットトンネリングを有効にすると、DNS 要求は宛先アドレスに基づいて送信されます。スプリットトンネリングを有効にしていない場合、DNS 要求はすべて保護された接続を介します。
  - [常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）]：スプリットトンネリングを有効にするが、すべての DNS 要求を保護された接続を介して、グループで定義された DNS サーバーに送信する場合は、このオプションを選択します。

- [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）]：保護された DNS サーバーが特定のドメインのアドレスだけを解決するようにする場合は、このオプションを選択します。次に、ドメインを指定します。ドメイン名はコンマで区切ります。例：example.com, example1.com。内部 DNS サーバーが内部ドメインの名前を解決し、外部 DNS サーバーが他のすべてのインターネットトラフィックを処理するようにする場合は、このオプションを使用します。

AnyConnect 属性

グループポリシーの AnyConnect 属性は、AnyConnect クライアントでリモートアクセス VPN 接続に使用されるいくつかの SSL および接続設定を定義します。

- **SSL 設定**
  - [Datagram Transport Layer Security（DTLS）の有効化（Enable Datagram Transport Layer Security (DTLS)）]：AnyConnect クライアントが SSL トンネルと DTLS トンネルの 2 つのトンネルを同時に使用することを許可するかどうかを指定します。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。DTLS をイネーブルにしない場合、SSL VPN 接続を確立している AnyConnect クライアント ユーザーは SSL トンネルのみで接続します。
  - [DTLS圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）接続を圧縮するかどうかを指定します。[DTLS圧縮（DTLS Compression）] はデフォルトで無効になっています。
  - [SSL圧縮（SSL Compression）]：データ圧縮を有効にするかどうかを指定します。有効にする場合、使用するデータ圧縮の方法は（[圧縮（Deflate）] または [LZS]）です。[SSL圧縮（SSL Compression）] はデフォルトで無効になっています。データ圧縮により、伝送速度は上がりますが、各ユーザーセッションのメモリ要件と CPU 使用率も高くなるため、SSL 圧縮はデバイスの全体的なスループットを低下させます。
  - [SSLキーの再生成方法（SSL Rekey Method）]、[SSLキーの再生成間隔（SSL Rekey Interval）]：クライアントは、暗号キーと初期化ベクトルを再ネゴシエーションしながら VPN 接続キーを再生成して、接続のセキュリティを強化します。[なし（None）] を選択して、キーの再生成を無効にします。キーの再生成を有効にするには、新しいトンネルを作成するたびに [新しいトンネル（New Tunnel）] を選択します（[既存のトンネル（Existing Tunnel）] オプションは、[新しいトンネル（New Tunnel）] と同じアクションになります）。キーの再生成を有効にする場合は、キーの再生成間隔も設定します。デフォルトは 4 分です。間隔は、4 ～ 10080 分（1 週間）の範囲で設定できます。
- **接続の設定**
  - [DF（Don't Fragment）ビットを無視する（Ignore the DF (Don't Fragment) 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を指定します。DF ビットが設定されているパケットの強制フラグメンテーションを許可し、

それらのパケットがトンネルを通過できるようにするには、このオプションを選択します。

- [Client Bypass Protocol]：セキュアゲートウェイによる（IPv6 トラフィックだけを予期しているときの）IPv4 トラフィックの管理方法や、（IPv4 トラフィックだけを予期しているときの）IPv6 トラフィックの管理方法を設定できます。

  AnyConnect クライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが AnyConnect 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合、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、Client Bypass Protocol 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）を設定できます。

  たとえば、セキュア ゲートウェイが AnyConnect 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [MTU]：Cisco AnyConnect VPN Client 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 バイトで、範囲は 576 ー 1462 バイトです。

  - [AnyConnectとVPNゲートウェイ間のキープアライブメッセージ（Keepalive Messages Between AnyConnect and VPN Gateway）]：トンネルでのデータの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。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。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。

  - [ゲートウェイ側の間隔でのDPD（DPD on Gateway Side Interval）]、[クライアント側の間隔でのDPD（DPD on Client Side Interval）]：ピアが応答しなくなったときに VPN ゲートウェイまたは VPN クライアントによる迅速な検出を確実に実行するには、Dead Peer Detection（DPD; デッドピア検出）を有効にします。ゲートウェイまたはクライアント DPD を個別に有効にすることができます。DPD メッセージのデフォルトの送信間隔は 30 秒です。間隔は、5～3600 秒にすることができます。

トラフィック フィルタ属性

グループポリシーのトラフィックフィルタ属性は、グループに割り当てられているユーザーに適用する制限を定義します。アクセス コントロール ポリシー ルールを作成する代わりにこれらの属性を使用することで、ホストまたはサブネットアドレスとプロトコル、または VLAN に基づいて、RA VPN ユーザーのアクセスを特定のリソースに制限できます。デフォルトで

は、RA VPN ユーザーは、保護されたネットワーク上の宛先へのアクセスがグループポリシーによって制限されることはありません。

- [アクセスリストフィルタ（Access List Filter）]：拡張アクセス制御リスト（ACL）を使用してアクセスを制限します。Smart CLI 拡張 ACL オブジェクトを選択します。拡張 ACL では、送信元アドレス、宛先アドレス、およびプロトコル（IP や TCP など）に基づいてフィルタリングできます。ACL はトップダウン方式で最初に一致したものから評価されるため、具体的なルールはより一般的なルールの前に配置してください。ACL の末尾には、暗黙的な「deny any」があるため、いくつかのサブネットへのアクセスを拒否しながら、他のすべてのアクセスを許可する場合は、ACL の最後に「permit any」ルールを含めてください。拡張 ACL スマート CLI オブジェクトを編集しながらネットワークオブジェクトを作成することはできないため、グループポリシーを編集する前に、ACL を作成する必要があります。そうしないと、単純にオブジェクトを作成し、後でもう一度ネットワークオブジェクトを作成し、その後で必要なすべてのアクセス制御エントリを作成する必要があります。ACL を作成するには、FDM にログインして、**[デバイス]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト]** に移動し、オブジェクトを作成して、オブジェクトタイプとして [拡張アクセスリスト（Extended Access List）] を選択します。

- [VPNをVLANに制限（Restrict Access to VLAN）]：「VLAN マッピング」とも呼ばれるこの属性で、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 インターフェイスを指定します。システムは、このグループからのトラフィックすべてを、選択した 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。デバイスのサブインターフェイスで定義されている VLAN 番号を指定していることを確認します。値の範囲は 1 ～ 4094 です。

Windows ブラウザ プロキシ属性

グループポリシーの Windows ブラウザプロキシ属性は、ユーザーのブラウザで定義されたプロキシが動作しているかどうか、およびその動作方法を判断します。

[VPNセッション中のブラウザプロキシ（Browser Proxy During VPN Session）] に対して次のいずれかの値を選択できます。

- [エンドポイント設定のまま（No change in endpoint settings）]：HTTP のブラウザプロキシを設定するかどうかをユーザーが決定できます。設定されている場合、そのプロキシが使用されます。

- [ブラウザプロキシの無効化（Disable browser proxy）]：ブラウザに定義されているプロキシ（ある場合）を使用しません。どのブラウザ接続もプロキシを経由しません。

- [自動検出設定（Auto detect settings）]：クライアントデバイスのブラウザでの自動プロキシサーバー検出の使用を有効にします。

- [カスタム設定を使用（Use custom settings）]：HTTP トラフィックに対してすべてのクライアントデバイスで使用する必要があるプロキシを定義します。次を設定します。

- [プロキシサーバーのIPまたはホスト名（Proxy Server IP or Hostname）]、[ポート]：プロキシサーバーの IP アドレスまたはホスト名、およびプロキシサーバーが使用するプロキシ接続のポート。ホストとポートを組み合わせた文字数が 100 文字を超えることはできません。
- [ブラウザプロキシ免除リスト（Browser Proxy Exemption List）]：免除リストにあるホスト/ポートへの接続はプロキシを経由しません。プロキシを使用すべきでない宛先のすべてのホスト/ポート値を追加します。例：www.example.com ポート 80。[プロキシ例外の追加（Add proxy exception）] をクリックしてリストに項目を追加します。項目を削除するには、ごみ箱アイコンをクリックします。すべてのアドレスとポートを合わせたプロキシ例外リスト全体で、255 文字を超えることはできません。

ASA RA VPN 設定の作成

CDO を使用して、1 つ以上の適応型セキュリティアプライアンス（ASA）デバイスを RA VPN 設定ウィザードに追加し、デバイスに関連付けられた VPN インターフェイス、アクセス制御、および NAT 免除設定ができます。したがって、各 RA VPN 設定には、RA VPN 設定に関連付けられた複数の ASA デバイス間で共有される接続プロファイルとグループポリシーを含めることができます。さらに、接続プロファイルとグループポリシーを作成して、設定を拡張できます。

RA VPN 設定がすでになされている ASA デバイス、または RA VPN 設定のない新しいデバイスを導入準備できます。「ASA デバイスの導入準備」を参照してください。RA VPN 設定がすでにある ASA デバイスを導入準備すると、CDO は自動的に「デフォルトの RA VPN 設定」を作成し、ASA デバイスをこの設定に関連付けます。このデフォルト設定には、デバイスで定義されているすべての接続プロファイルオブジェクトを含めることができます。詳細については、「オンボーディング済み ASA デバイスの RA VPN 設定の読み取り」を参照してください。CDO では、デフォルトの設定を削除できます。

重要

- 同じリモートアクセス VPN 設定に ASA と FTD を追加することは許可されていません。
- ASA デバイスは、1 つ以上の RA VPN 設定を持つことはできません。

始める前に

ASA デバイスを RA VPN 設定に追加する前に、ASA デバイスで次の前提条件が満たされている必要があります。

- ライセンス要件

  輸出規制されている機能に対して、デバイスを有効にする必要があります。

  ASA デバイスのライセンスの概要を表示するには、ASA コマンド ライン インターフェイスで show license summary コマンドを実行します。CDO ASA CLI インターフェイスを使用するには、「CDO インターフェイスでの ASA CLI の使用」を参照してください。

  - ライセンスの概要で有効になっている輸出規制機能の例：

```
Registration: Status: REGISTERED Smart Account: Cisco SVS temp-request access
licensing@cisco.com Export-Controlled Functionality: ALLOWED

Last Renewal Attempt: None

Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
```

VPN 設定を作成または編集するには、[エクスポート制御機能（Export-Controlled Functionality）] プロパティを [許可（Allowed）] ステータスにする必要があります。

このプロパティが [許可しない（Not Allowed）] ステータスの場合、VPN 設定を作成または変更する際に CDO がエラーメッセージ（「エクスポートに準拠していないデバイスには RA VPN を設定できません」）を表示し、デバイスの RA VPN 設定を許可しません。

- デバイスのID 証明書

  証明書は、クライアントと ASA デバイス間の接続を認証するために必要です。VPN 設定を開始する前に、ID 証明書が ASA デバイスにすでにあることを確認してください。

  証明書がデバイスにあるかどうかを確認するには、ASA コマンド ライン インターフェイスで **show crypto CA Certificates** コマンドを実行します。CDO ASA CLI インターフェイスを使用するには、「CDO インターフェイスでの ASA CLI の使用」を参照してください。

  ID 証明書がない場合、または新しい証明書に登録する場合は、CDO を使用してそれらを ASA にインストールします。ASA 証明書管理を参照してください。

  リモートアクセス VPN コンテキストでのデジタル証明書の使用については、リモートアクセス VPN 認証ベースの認証 （126 ページ）で説明されています。

- 外部インターフェイス

  外部インターフェイスが、ASA デバイスですでに設定されている必要があります。**インターフェイスを設定するには、ASDM または ASA CLI を使用する必要があります。**ASDM を使用したインターフェイスの設定については、『Cisco ASA Series General Operations CLI Configuration Guide, XY』の「Interfaces」ブックを参照してください。

- AnyConnect パッケージをダウンロードして、リモートサーバーにアップロードします。その後、RA VPN ウィザードまたは ASA ファイル管理ウィザードを使用して、AnyConnect ソフトウェアパッケージをサーバーから ASA にアップロードします。手順については、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

- 保留中の設定展開はありません。

- 認証にローカルデータベースを使用している場合、ASDM または ASA CLI を使用して、ローカルデータベースにユーザーアカウントを追加します。

  ASDM を使用してユーザーアカウントを追加するには、『Cisco ASA Series VPN CLI Configuration Guide, X.Y』の「AAA Servers and the Local Database」ブックの「Add a User Account to the Local Database」セクションを参照してください。

  ASA CLI を使用してユーザーアカウントを追加するには、**username[***username***] password [***password***] privilege [***priv_level***]** コマンドを実行します。

- ASA の変更は CDO に同期されます。

1. 左側の CDO ナビゲーションバーで、[デバイスとサービス] をクリックし、同期する 1 つ以上の ASA デバイスを検索します。
2. 1 つ以上のデバイスを選択し、[変更の確認（Check for changes）] をクリックします。CDO は 1 つ以上の FTD デバイスと通信して、変更を同期します。

- RA VPN 設定グループポリシーのオブジェクトは一貫しています。
  - 一貫性のないすべてのグループポリシーのオブジェクトは RA VPN 設定に追加できないため、それらが解決されていることを確認します。問題に対処するか、一貫性のないグループポリシーのオブジェクトを [オブジェクト] ページから削除します。詳細については、「重複オブジェクト問題の解決」および「一貫性のないオブジェクト問題の解決」を参照してください。

ステップ 1 ASA デバイスの導入準備。

ステップ 2 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]**をクリックします。

ステップ 3 青いプラス  ボタンをクリックして、新しい RA VPN 設定を作成します。

ステップ 4 リモートアクセス VPN の設定の名前を入力します。

ステップ 5 青いプラス  ボタンをクリックして、ASA デバイスを設定に追加します。

デバイスの詳細を追加し、デバイスに関連付けられたネットワークトラフィック関連の権限を設定できます。

1. 次のデバイスの詳細を提供します。
   - [デバイス]：追加する ASA デバイスを選択し、[選択（Select）] をクリックします。**重要**：同じリモートアクセス VPN 設定に ASA と FTD を追加することはできません。
   - [デバイス ID 証明書（Certificate of Device Identity）]：デバイスのアイデンティティを確立するために使用する内部証明書を選択します。内部証明書は、AnyConnect クライアントがデバイスへの接続を行うときにデバイスのアイデンティティを確立します。クライアントはこの証明書を承認して、セキュアな VPN 接続を完了させる必要があります。
   - [外部インターフェイス（Outside Interface）]：リモートアクセス VPN 接続を確立するときにユーザーが接続するインターフェイスを選択します。これは通常外部（インターネットに接続された）インターフェイスですが、デバイスとこの接続プロファイルがサポートしているエンドユーザー間のインターフェイスのいずれかを選択します。

     注目 エクスポートに準拠していないデバイスの RA VPN 設定を作成または変更することはできません。輸出規制機能が有効になっている ASA デバイスのライセンスを取得して、再試行する必要があります。

2. [続行] をクリックして、トラフィックの権限を設定します。

- [暗号解読されたトラフィック（sysopt permit-vpn）に対するバイパスアクセス コントロール ポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、暗号解読されたトラフィックは、アクセス コントロール ポリシーのインスペクションの対象になります。このオプション[複合されたトラフィックのバイパス（bypasses the decrypted traffic）]オプションを有効にすると、アクセス コントロール ポリシーのインスペクションがバイパスされますが、AAA サーバーからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。

  このオプションを選択すると、システムによりグローバル設定である sysopt connection permit-vpn コマンドが設定されることに注意してください。これは、サイト間 VPN 接続の動作にも影響を及ぼします。

  このオプションを選択しない場合、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングし、ネットワークにアクセスするおそれがあります。この理由は、アドレスプールに内部リソースへのアクセスを許可するアクセス制御ルールを作成する必要があるためです。アクセス制御ルールを使用する場合は、送信元 IP アドレスだけではなく、ユーザーの仕様を使用してアクセスを制御することを検討してください。

  このオプションを選択することの欠点は、VPN トラフィックが検査されないことです。つまり、侵入およびファイル保護、URL フィルタリング、またはその他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

- [NAT免除（NAT Exempt）]：NAT 免除を使用すると、アドレスは変換から除外され、変換済みのホストとリモートホストの両方が保護されたホストとの接続を開始できるようになります。リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を設定します。NAT からの ASA リモート アクセス トラフィックの除外 （127 ページ）を参照してください。

3. [OK] をクリックします。

   [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）]には、デバイスですでに使用可能な AnyConnect パッケージが表示されます。

   RA VPN ウィザードから AnyConnect パッケージを ASA にアップロードするには、次の 2 つのオプションがあります。

   - （オプション 1）：CDO のリポジトリからパッケージを選択します。ASA はインターネットにアクセスできる必要があります。
   - （オプション 2）：AnyConnect パッケージがプリロードされている ftp/http/https/scp/smb/tftp URL の場所を指定します。

   手順については、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

   （注） 注:既存のパッケージを置き換える場合は、「ASA デバイス上の AnyConnect ソフトウェアパッケージの管理」を参照してください。

ステップ 6 [OK] をクリックします。

ASA VPN 設定が作成されます。

ASA RA VPN 構成の変更

既存の RA VPN 構成の名前とデバイスの詳細を変更できます。

ステップ 1 変更する構成を選択し、[アクション] の下で [編集] をクリックします。

- 必要に応じて名前を変更します。
- 青色のプラス  ボタンをクリックして、新しいデバイスを追加します。
- をクリックして、ASA デバイスで次の手順を実行します。
  - [編集] をクリックして、既存の RA VPN 構成を変更します。
  - [削除] をクリックして、RA VPN 構成から ASA デバイスを削除します。グループポリシーを除き、そのデバイスに関連付けられているすべての接続プロファイルと RA VPN 設定が削除されます。グループポリシーは、オブジェクトページから明示的に削除できます。

    （注） 構成を使用しているデバイスがその ASA だけの場合は、ASA を削除できません。代わりに、RA VPN 構成を削除できます。

ステップ 2 CDO から ASA に設定変更を展開します。

次のタスク

構成またはデバイスの名前を入力して、リモートアクセス VPN 構成を検索することもできます。

関連情報：

- ASA RA VPN 接続プロファイルの設定 （109 ページ）。

ASA RA VPN 接続プロファイルの設定

リモートアクセスVPN接続プロファイルの定義する接続特性では、外部ユーザーがAnyConnectクライアントを使用してシステムにVPN接続することを許可します。各プロファイルは、ユーザーの認証に使用される AAA サーバーと証明書、ユーザーの IP アドレスを割り当てるためのアドレスプール、およびさまざまなユーザー関連の属性を定義するグループポリシーを定義します。

異なるユーザーグループに異なるサービスを提供する必要がある場合、または異なる認証ソースがある場合は、RA VPN 設定内に複数のプロファイルを作成できます。たとえば、自分の組

織が異なる認証サーバーを使用する別の組織とマージする場合、別の組織の認証サーバーを使用する新しいグループのプロファイルを作成できます。

RA VPN 接続プロファイルを作成すると、ユーザーは、ホームネットワークなどの外部ネットワークから内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。

始める前に

ASA RA VPN 設定の作成 （105 ページ）。

ステップ 1 CDO ナビゲーションウィンドウで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]** をクリックします。VPN 設定をクリックして、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報を表示できます。

（注） デバイスに割り当てられているグループポリシーを確認するには、[アクション] で [グループポリシー（Group Policies）] をクリックします。接続プロファイルに割り当てられたグループポリシーは、リストに自動的に追加され、削除できません。

必要なグループポリシーがまだ存在しない場合は、  をクリックしてリストから選択します。必要なサービスを提供するために追加のグループポリシーを作成することができます。「新規 ASA RA VPN グループポリシーの作成 （96 ページ）」を参照してください。

ステップ 2 接続プロファイルをクリックし、右側のサイドバーの [アクション] で [接続プロファイルの追加（Add Connection Profile）] をクリックします。

ステップ 3 基本接続の属性を設定します。

- [接続プロファイル名（Connection Profile Name）]：スペースを含めずに最大 50 文字で、この接続の名前を指定します。例、MainOffice。

  （注） ここで入力する名前が、AnyConnect クライアントの接続リストに表示されます。ユーザーにとって意味のある名前を選択します。

- [グループエイリアス（Group Alias）]、[グループURL（Group URL）]：エイリアスには特定の接続プロファイルの代替名または URL が含まれます。VPN ユーザーは、 ASA デバイスへの接続時に、接続リストの AnyConnect クライアントでエイリアス名を選択できます。接続プロファイル名はグループのエイリアスとして自動的に追加されます。グループ URL のリストも設定できます。このリストは、リモートアクセス VPN 接続を開始するときにエンドポイントが選択できるリストです。ユーザーがグループ URL を使用して接続すると、システムはその URL に一致する接続プロファイルを自動的に使用します。この URL は、AnyConnect クライアントをまだインストールしていないクライアントによって使用されます。グループエイリアスと URL を必要な数だけ追加します。これらのエイリアスと URL は、デバイスで定義されているすべての接続プロファイルで一意である必要があります。グループ URL は https:// で始まる必要があります。

- たとえば、エイリアスは Contractor、グループ URL は https://ravpn.example.com/contractor のように指定できます。AnyConnect クライアントをインストールすると、ユーザーは単純に AnyConnect VPN の接続ドロップダウンリストでグループエイリアスを選択します。

ステップ 4 プライマリ アイデンティティ ソース、および必要に応じてセカンダリ ソースを設定します。これらのオプションにより、リモートアクセス VPN 接続を有効にするための、デバイスへのユーザー認証方法が決定されます。最も簡単なアプローチは、AAA のみを使用し、AD レルムを選択するか、または LocalIdentitySource を使用する方法です。[認証タイプ] として次のアプローチを使用できます。

- [AAAのみ（AAA Only）]：ユーザー名とパスワードに基づいてユーザーを認証および認可します。詳細は、接続プロファイルのための AAA の設定 （111 ページ）を参照してください。
- [クライアント証明書のみ]：クライアント デバイス ID 証明書に基づいてユーザーを認証します。詳細については、「接続プロファイルの証明書認証の設定」を参照してください。
- [AAAおよびクライアント認証（AAA and Client Certificate）]：ユーザー名/パスワードと、クライアント デバイス ID 証明書の両方を使用します。

ステップ 5 クライアントのアドレスプールを設定します。アドレスプールは、リモートクライアントが VPN 接続を確立するときに、システムがリモートクライアントに割り当てることができる IP アドレスを定義します。詳細については、「クライアントアドレスプール割り当ての設定」を参照してください。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 リストからこのプロファイルに対して使用する [グループポリシー（Group Policy）] を選択し、[選択（Select）] をクリックします。

グループポリシーは、トンネル確立後のユーザー接続の期間を設定します。システムには、「DfltGrpPolicy」という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。「新規 ASA RA VPN グループポリシーの作成（96 ページ）」を参照してください。

ステップ 8 [続行（Continue）] をクリックします。

ステップ 9 サマリーを確認します。最初に、サマリーが正しいことを確認します。AnyConnect ソフトウェアをインストールし、VPN 接続を完了できることをテストするために、エンドユーザーが最初に行う必要がある内容を確認できます。 をクリックしてこれらの手順をクリップボードにコピーし、ユーザーに配布します。

ステップ 10 [完了（Done）] をクリックします。

ステップ 11 「ASA のエンドツーエンド リモート アクセス VPN 設定プロセス」のステップ 5 を実行します。

接続プロファイルのための AAA の設定

認証、許可、およびアカウンティング（AAA） サーバーは、ユーザー名とパスワードを使用して、ユーザーのリモートアクセス VPN へのアクセスを許可するかどうかを判断します。RADIUS サーバーを使用する場合は、認証されたユーザー間で許可レベルを区別して、保護されたリソースへの差別化されたアクセスを提供できます。使用状況を追跡するために RADIUS アカウンティングサービスを使用することもできます。

AAA を設定する場合は、プライマリ アイデンティティ ソースを設定する必要があります。セカンダリ ソースとフォールバック ソースはオプションです。RSA トークンや DUO などを使用する二重認証を実装する場合は、セカンダリ ソースを使用します。

プライマリ アイデンティティ ソースのオプション

- [ユーザー認証用のプライマリアイデンティティソース]：認証はユーザーを特定する方法です。アクセスが許可されるには、ユーザーは通常、有効なユーザー名と有効なパスワードを入力する必要があります。プライマリ アイデンティティ ソースはリモートユーザーを認証する目的で使用されます。VPN接続を完了するには、エンドユーザーがこのソースか任意のフォールバックソースで定義されている必要があります。次のいずれかを選択します。
  - Active Directory（AD）のアイデンティ レルム。
  - RADIUS サーバーグループ。
  - LocalIdentitySource（ローカル ユーザー データベース）：デバイスで直接ユーザーを定義できます。外部サーバーを使用することはできません。

    ASA のアイデンティティソースを設定するをクリックすると、新しいアイデンティティソースを作成できます。

- [フォールバックローカルアイデンティティソース]：プライマリソースが外部サーバーの場合、プライマリサーバーが使用できない場合のフォールバックとしてLocalIdentitySourceを選択できます。フォールバック ソースとしてローカルデータベースを使用する場合は、必ず外部サーバで定義したものと同じローカル ユーザ名/パスワードを定義します。
- [削除オプション]：レルムとは管理ドメインのことです。次のオプションを有効にすると、ユーザー名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
  - [ユーザー名からアイデンティティソースサーバーを削除]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からアイデンティティソース名を削除するかどうか。たとえば、このオプションを選択してユーザーが「username」として domain\username に入ると、ユーザー名からドメインが削除され、認証用の AAA サーバーに送信されます。デフォルトでは、このオプションはオフになります。
  - [ユーザー名からグループを削除]：ユーザー名をAAAサーバーに渡す前に、ユーザー名からグループを削除するかどうか。このオプションは、username@domain形式で指定された名前に適用されます。選択すると、domainと@記号が削除されます。デフォルトでは、このオプションはオフになります。

セカンダリ アイデンティティ ソース

- [ユーザー承認用のセカンダリアイデンティティソース]：オプションの 2 番目のアイデンティティソースです。ユーザーがプライマリソースで正常に認証されると、セカンダリソースでの認証が求められます。AD レルム、RADIUS サーバーグループ、またはローカル アイデンティティ ソースを選択することができます。
- [詳細オプション]：[詳細] リンクをクリックし、次のオプションを設定します。

- [セカンダリ用フォールバックローカルアイデンティティソース（Fallback Local Identity Source for Secondary）]：セカンダリソースが外部サーバーの場合、セカンダリサーバーが使用できない場合のフォールバックとしてLocalIdentitySourceを選択できます。フォールバックソースとしてローカルデータベースを使用する場合は、必ずセカンダリ外部サーバーで定義したものと同じローカルユーザー名/パスワードを定義します。
- [セカンダリログインにプライマリユーザー名を使用]：デフォルトでは、セカンダリアイデンティティ ソースを使用する場合、セカンダリ ソースに対してユーザー名とパスワードの両方が求められます。このオプションを選択すると、システムはセカンダリパスワードの入力のみを求め、プライマリ アイデンティティ ソースに対して認証されたものと同じユーザー名をセカンダリソースに対して使用します。プライマリとセカンダリの両方のアイデンティティソースで同じユーザー名を設定する場合は、このオプションを選択します。
  - [セッションサーバーのユーザー名]：認証に成功すると、ユーザー名はイベントと統計ダッシュボードに表示されます。ユーザー名はユーザーベースまたはグループベースのSSL暗号解読化およびアクセス制御ルールに一致するものを判断するために使用され、アカウンティングに使用されます。2 つの認証ソースを使用しているため、ユーザーアイデンティティとして、プライマリまたはセカンダリのどちらのユーザー名を使用するのかシステムに通知する必要があります。デフォルトでは、プライマリ名が使用されます。
  - [パスワードタイプ]：セカンダリサーバーのパスワードを取得する方法。デフォルトは[プロンプト（Prompt）]で、ユーザーはパスワードの入力が求められることを意味します。プライマリサーバーへのユーザー認証時に入力したパスワードを自動的に使用するには、[プライマリアイデンティティソースのパスワード（Primary Identity Source Password）]を選択します。すべてのユーザーに同じパスワードを使用するには[共通パスワード]を選択し、[共通パスワード]フィールドにそのパスワードを入力します。
- [承認サーバー]：リモートアクセスVPNユーザーを認証するように設定されたRADIUSサーバーグループです。認証の完了後、認可によって、認証済みの各ユーザーが使用できるサービスおよびコマンドが制御されます。認可は、ユーザーが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザーに対して同じアクセス権を提供します。

  システムがグループポリシーで定義されているものと重複する認可属性を RADIUS サーバーから取得した場合、RADIUS 属性は、グループポリシー属性をオーバーライドすることに注意してください。

  [RADIUSサーバーグループの作成（Create RADIUS Server Group）]をクリックして、新しいサーバーグループを作成できます。ASA RADIUS サーバーオブジェクトまたはグループの作成または編集 （94 ページ）
- [アカウンティングサーバー]：（オプション）リモートアクセスVPNセッションへのアカウンティングに使用するRADIUSサーバーグループ。アカウンティングは、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワークリソース

の数を追跡します。ASA デバイスは、RADIUS サーバーにユーザーアクティビティを報告します。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

[RADIUSサーバーグループの作成（Create RADIUS Server Group）] をクリックして、新しいサーバーグループを作成できます。ASA RADIUS サーバーオブジェクトまたはグループの作成または編集 （94 ページ）

接続プロファイルのための証明書認証の設定

（注） このセクションは、**認証タイプ**が **AAA のみ**の場合には適用されません。

リモート アクセス VPN 接続を認証するために、クライアント デバイスにインストールされた証明書を使用することができます。

クライアント証明書を使用していても、セカンダリ アイデンティティ ソース、フォールバック ソース、および認証およびアカウンティングサーバーを引き続き設定できます。これらは AAA オプションです。詳細については ASA RA VPN 接続プロファイルの設定 （109 ページ）を参照してください。

次に、証明書固有の属性を示します。これらの属性は、プライマリ アイデンティティ ソースとセカンダリ アイデンティティ ソースに対して個別に設定できます。セカンダリ ソースの設定はオプションです。

- [証明書のユーザー名]：次のいずれかを選択します。
  - [マップ固有フィールド]：証明書の要素を [プライマリフィールド] および [セカンダリフィールド] の順番で使用します。デフォルトは CN（共通名）と OU（組織単位）です。組織に適したオプションを選択します。これらのフィールドを組み合わせてユーザー名が提供され、このユーザー名がイベント、ダッシュボード、さらに SSL 暗号解読とアクセス制御ルールでのマッチング目的に使用されます。
  - [DN（識別名）全体をユーザー名として使用]：システムが自動的に DN フィールドからユーザー名を導出します。
- [詳細オプション]：（[認証タイプ] が [クライアント証明書のみ] の場合には適用されません）：[詳細] リンクをクリックし、次のオプションを設定します。
  - [ユーザーログインウィンドウの証明書からユーザー名を事前入力]：ユーザーに認証を要求するときに、取得したユーザー名をユーザー名フィールドに入力するかどうか。

- [ログインウィンドウでユーザー名を非表示にする]：[事前入力] オプションを選択すると、ユーザー名を非表示にできます。これは、ユーザーがパスワードプロンプトでユーザー名を編集できないことを意味します。

クライアントアドレスプール割り当ての設定

リモートアクセス VPN に接続するエンドポイントにシステムが IP アドレスを提供するための方法が必要です。AAA サーバーは、これらのアドレス、DHCP サーバー、グループポリシーで設定されている IP アドレスプール、または接続プロファイルで設定された IP アドレスプールを提供できます。システムは、この順序でこれらのリソースを試行し、使用可能なアドレスを取得すると停止し、次にアドレスをクライアントに割り当てます。このように、同時接続数が異常な場合のフェールセーフを作成するために複数のオプションを設定できます。

接続プロファイルのアドレスプールを設定するには、次の方法の 1 つ以上を使用します。

- [IPv4アドレスプール] および [IPv4アドレスプール]：まず、サブネットを指定する最大 6 つのネットワークオブジェクトを作成します。IPv4 と IPv6 に別々のプールを設定できます。次に、グループポリシーまたは接続プロファイルの [IPv4アドレスプール] および [IPv6アドレスプール] オプションで、これらのオブジェクトを選択します。IPv4 と IPv6 の両方を設定する必要はありません。サポートするアドレス方式を設定してください。また、グループポリシーと接続プロファイルの両方でプールを設定する必要もありません。グループポリシーは接続プロファイル設定をオーバーライドします。そのため、グループポリシーでプールを設定する場合は、接続プロファイルのオプションを空白のままにしてください。プールはリストの順序で使用されることに注意してください。新しい IPv4 または IPV6 アドレスプールを作成するには、「IP アドレスプールの作成」を参照してください。
- [DHCPサーバー]：まず、1 つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバーを設定します（DHCP を使用して IPv6 プールを設定することはできません）。次に、DHCP サーバーの IP アドレスを使用してホスト ネットワーク オブジェクトを作成します。その後、このオブジェクトは接続プロファイルの [DHCPサーバー（DHCP Servers）] 属性で選択できます。複数の DHCP サーバーを設定することができます。DHCP サーバーに複数のアドレスプールがある場合、[DHCPスコープ] 属性を接続プロファイルにアタッチする新規 ASA RA VPN グループポリシーの作成で使用して、使用するプールを選択することができます。プールのネットワークアドレスを使用して、ホスト ネットワーク オブジェクトを作成します。たとえば、DHCP プールに 192.168.15.0/24 および 192.168.16.0/24 が含まれている場合、DHCP スコープを 192.168.16.0 に設定すると、192.168.16.0/24 サブネットからのアドレスが必ず選択されるようになります。

関連情報：

ASA のエンドツーエンド リモート アクセス VPN 設定プロセス

ASA デバイス上の *AnyConnect* ソフトウェアパッケージの管理

次のいずれかの手順を実行して、リモートアクセス VPN ウィザードを使用して AnyConnect パッケージをアップロードできます。

- CDO リポジトリからパッケージをアップロードします。

- HTTP、HTTPS、TFTP、FTP、SMB、または SCP プロトコルを使用して、サーバーからパッケージをアップロードします。

CDO リポジトリから AnyConnect パッケージをアップロードする

リモートアクセス VPN 設定ウィザードには、CDO リポジトリからオペレーティングシステムごとに AnyConnect パッケージが表示されるため、選択してデバイスにアップロードできます。デバイスがインターネットにアクセスでき、DNS が適切に設定されていることを確認してください。

（注） 目的のパッケージが表示されたリストにない場合、またはデバイスがインターネットにアクセスできない場合は、AnyConnect パッケージがプリロードされているサーバーを使用してパッケージをアップロードできます。

ステップ 1 オペレーティングシステムに対応するフィールドをクリックし、AnyConnect パッケージを選択します。

ステップ 2 をクリックして、パッケージをアップロードします。チェックサムが一致しない場合、AnyConnect パッケージのアップロードは失敗します。失敗の詳細については、デバイスの [ワークフロー（workflow）] タブで確認できます。

サーバーから ASA への AnyConnect パッケージのアップロード

AnyConnect クライアント ソフトウェア パッケージをコンピュータにダウンロードし、ASA からアクセス可能なリモートサーバーにそれをアップロードします。その後、RA VPN ウィザードまたは ASA ファイル管理ウィザードを使用して、そのサーバーから ASA に AnyConnect ソフトウェアパッケージをアップロードします。ドメイン名を使用する URL 用に、デバイスで DNS を正しく設定する必要があります。

ASA RA VPN ウィザードは、HTTP、HTTPS、TFTP、FTP、SMB、SCP プロトコルを使用したパッケージのアップロードをサポートしています。

ファイルのアップロード時にサポートされているプロトコルの構文:

プロトコル（Protocol）	構文	例
HTTP	http://[[パス/]ファイル名]	http://www.geonames.org/data-sources.html
HTTPS	https://[[パス/]ファイル名]	https://docs.aws.amazon.com/amazon/tagging.html
TFTP	tftp://[[パス/]ファイル名]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[ユーザー[:パスワード]@]サーバー[:ポート]/[パス/]ファイル名]	[illegible]
SMB	smb://[[パス/]ファイル名]	smb://10.10.32.145//sambashare/hello.txt

プロトコル（Protocol）	構文	例
SCP	scp://[[ユーザー[:パスワード]@]サーバー[/パス]/ファイル名]	scp://rootcisco123@10.10.10.166/root/events_send.py

始める前に

必要なオペレーティングシステム用の「AnyConnect ヘッドエンド展開パッケージ」をダウンロードしていることを確認してください。最新の機能、バグ修正、セキュリティパッチを確保するには、常に最新の AnyConnect バージョンをダウンロードする必要があります。デバイスのパッケージは定期的に更新してください。

重要 ASA ファイル管理ウィザードを使用してパッケージをアップロードすることを選択した場合、パッケージのダウンロード後に名前を変更しないでください。

（注） オペレーティングシステム（OS）（Windows、Mac、Linux）ごとに 1 つの AnyConnect をアップロードできます。1 つの OS タイプに対して複数のバージョンをアップロードすることはできません。

ステップ 1 https://software.cisco.com/download/home/283000185 から AnyConnect パッケージをダウンロードします。

- EULA に同意し、K9（暗号化されたイメージ）の権限を持っていることを確認してください。
- オペレーティングシステムの「AnyConnect ヘッドエンド展開パッケージ」を選択します。パッケージ名は「anyconnect-win-4.7.04056-webdeploy-k9.pkg」のようになります。Windows、macOS、Linux のそれぞれに個別のヘッドエンドパッケージがあります。

ステップ 2 AnyConnect パッケージをリモートサーバーにアップロードします。ASA デバイスとサーバーからのネットワークルートがあることを確認します。

ASA RA VPN ウィザードは、HTTP、HTTPS、TFTP、FTP、SMB、SCP プロトコルを使用したパッケージのアップロードをサポートしています。

重要 AnyConnect パッケージを HTTPS サーバーにアップロードする場合は、以下の手順を実行してください。

- そのサーバーの信頼できる CA 証明書を ASA デバイスにアップロードします。
- 信頼できる CA 証明書を HTTPS サーバーにインストールします。

ステップ 3 リモートサーバーの URL は、認証を求めない直接リンクである必要があります。URL が事前認証されている場合は、RA VPN ウィザードの URL を指定してファイルをダウンロードできます。

ステップ 4 リモートサーバーの IP アドレスが NAT 処理されている場合は、リモートサーバーのロケーションの NAT 処理済みパブリック IP アドレスを指定する必要があります。

AnyConnect パッケージの ASA へのアップロード

RA VPN ウィザードまたは ASA ファイル管理ウィザードを使用して、AnyConnect ソフトウェアパッケージを ASA にアップロードできます。

HTTP または HTTPS サーバーから ASA デバイスに新しい AnyConnect パッケージをアップロードするには、次の手順を使用します。

ステップ 1 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、Windows、Mac、Linux のエンドポイントに対して別々のパッケージをアップロードできます。

ステップ 2 対応するプラットフォームフィールドで、Windows、Mac、および Linux と互換性のある AnyConnect パッケージが事前にアップロードされているサーバーのパスを指定します。サーバーパスの例：
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'

ステップ 3 をクリックして、パッケージをアップロードします。CDO は、パスが到達可能であり、指定されたファイル名が有効なパッケージかどうかを検証します。検証が成功すると、AnyConnect パッケージの名前が表示されます。RA VPN 設定に ASA デバイスを追加して、AnyConnect パッケージをそれらにアップロードできます。

ステップ 4 [OK] をクリックします。AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 5 ステップ 5 から、「ASA RA VPN 設定の作成」に進みます。

次のタスク

VPN 接続を完了するには、ユーザーは AnyConnect クライアントソフトウェアをワークステーションにインストールする必要があります。詳細については、「ユーザーが AnyConnect クライアントソフトウェアを ASA にインストールする方法 」を参照してください。

ファイル管理ウィザードを使用した AnyConnect パッケージのアップロード

ファイル管理ウィザードを使用して、HTTP、HTTPS、TFTP、FTP、SMB、または SCP サーバーから単一または複数の ASA デバイスに AnyConnect パッケージをアップロードします。AnyConnect パッケージを複数の ASA デバイスに同時にプッシュする場合は、一括アップロードが便利です。詳細については、「ASA ファイルの管理」を参照してください。

重要 ASA ファイル管理ウィザードを使用してパッケージをアップロードすることを選択した場合、パッケージのダウンロード後に名前を変更しないでください。

アップロードが完了したら、ASA RA VPN 設定ウィザードを開き、パッケージが自動検出されることを確認します。1 つの OS バージョンに対して複数のパッケージをアップロードする場

合、ウィザードではそれらのパッケージがドロップダウンリストに表示され、そのリストの中から 1 つを選択できます。次に、RA VPN 設定を作成してデバイスに展開できます。

既存の AnyConnect パッケージの置換

AnyConnect パッケージがデバイスにすでに存在している場合、これらは RA VPN ウィザードに表示されます。オペレーティングシステムで利用可能なすべての AnyConnect パッケージが、ドロップダウンリストに表示されます。既存のパッケージをリストから選択して、新しいパッケージと置き換えることができます。ただし、新しいパッケージをリストに追加することはできません。

（注） 既存のパッケージを新しいパッケージに置き換える場合は、新しい AnyConnect パッケージが、ASA が到達できるネットワーク上のサーバーにすでにアップロードされていることを確認してください。

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPN（Remote Access VPN）]**をクリックします。

ステップ 2 変更する RA VPN 設定を選択し、[アクション] で [編集] をクリックします。

ステップ 3 [検出された AnyConnect パッケージ（AnyConnect Packages Detected）] で、既存の AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、置き換えるパッケージをリストから選択して [編集] をクリックします。既存のパッケージが対応するフィールドから消去されます。

ステップ 4 新しい AnyConnect パッケージがプリロードされているサーバーのパスを指定し、 をクリックしてパッケージをアップロードします。

ステップ 5 [OK] をクリックします。新しい AnyConnect パッケージが RA VPN 設定に追加されます。

ステップ 6 ステップ 6 から、「ASA RA VPN 設定の作成 （105 ページ）」に進みます。

AnyConnect パッケージの削除

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPN（Remote Access VPN）]**をクリックします。

ステップ 2 変更する RA VPN 設定を選択し、[アクション] で [編集] をクリックします。

ステップ 3 [検出されたAnyConnectパッケージ（AnyConnect Packages Detected）] で、削除する AnyConnect パッケージの横に表示される アイコンをクリックします。オペレーティングシステムに複数のバージョンの AnyConnect パッケージがある場合は、リストから削除するパッケージを選択します。既存のパッケージが対応するフィールドから消去されます。

（注） [キャンセル（Cancel）]をクリックすると削除操作を停止し、既存のパッケージが保持されます。

ステップ 4 [OK] をクリックします。 デバイスの [設定ステータス（Configuration Status）] は [未同期（Not Synced）] となります。

（注） この段階で削除アクションを取り消す場合は、[デバイスとサービス（Device & Services）] ページに移動し、[変更の破棄（Discard Changes）] をクリックして、既存の AnyConnect パッケージを保持します。

ステップ 5 CDO から ASA に設定変更を展開します。。

オンボーディング済み ASA デバイスの RA VPN 設定の読み取り

RA VPN 設定がすでに存在する ASDM 管理対象 ASA デバイスを導入準備すると、既存のリモートアクセス VPN 設定が検出されて表示されます。CDO は自動的に「デフォルトの RA VPN 設定」を作成し、ASA デバイスをこの設定に関連付けます。CDO では読み取られないか、サポートされていない RA VPN 設定がいくつかありますが、これらは、CDO コマンドライン インターフェイスで設定できます。

（注） このセクションでは、CDO でサポートされている設定またはサポートされていない設定についてすべては網羅していません。最も一般的に使用される設定のみを説明します。

導入準備した ASA の RA VPN 設定を表示するには、次の手順を実行します。

ステップ 1 CDO インターフェイスで、**[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）]** に移動します。

ステップ 2 導入準備した ASA デバイスに対応する RA VPN 設定をクリックします。CDO は自動的に「Default_RA_VPN_Configuration」を作成し、ASA デバイスをこの設定に関連付けます。デフォルト設定は削除できます。CDO で読み取られる ASA RA VPN 設定は、次のように分類されます。

- デバイス設定
- 接続プロファイル
- グループ ポリシー

デバイス設定

導入準備されている ASA デバイスに関連付けられている RA VPN 設定が **Default_RA_VPN_Configuration** に表示されます。この設定をクリックして、この設定に関連付けられている ASA デバイス（右側の [デバイス] ペインにあります）の名前 を表示する必要があります。編集ボタンをクリックして、ASA デバイスに存在する AnyConnect パッケージを表示することもできます。

接続プロファイル

CDO は、ASA デバイスの [AnyConnectクライアントVPNアクセス（AnyConnect Client VPN Access）] で定義された接続プロファイルをサポートしており、読み取ります。[クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] 設定はサポートしていません。

接続プロファイルの属性を確認するには、次の手順を実行します。

ステップ 1 **Default_RA_VPN_Configuration** を展開します。

ステップ 2 必要な接続プロファイルの 1 つをクリックし、[編集] をクリックします。

すべての基本および高度な ASA RA VPN 属性は、[CDO RA VPN] 設定ページの [接続プロファイル名と詳細（Connection Profile name and details）] に表示されます。

（注） デフォルトの設定を削除できます（デフォルトの RA VPN 設定を選択し、右側の [アクション] ペインで [削除] をクリックします）。

プライマリ アイデンティティ ソース

- CDO は、**接続エイリアス**属性と**グループ URL 属性**を**グループエイリアス**および**グループ URL** として読み取ります。

（注）
- SAML、複数の証明書と AAA、および複数の証明書を使用して設定された接続プロファイルは読み取られません。
- インターフェイスとサーバーグループを持つ認証サーバーグループはサポートされていません。

- CDO は、**プライマリ アイデンティティ ソース**で、「AAA」、「AAA と証明書」、「証明書のみ」の認証方式で設定された AnyConnect 接続プロファイルをサポートします。
- **AAA サーバーグループ**は、[プライマリ アイデンティティ ソース] で**ユーザー認証用のプライマリ アイデンティティ ソース**として CDO で読み取られます（この属性は、[認証タイプ] として [AAA] または [AAAとクライアント証明書] を選択することで表示できます）。
  - **AAA サーバーグループ**が LOCAL 以外に設定されている場合、CDO はこの属性を読み取り、[プライマリ アイデンティティ ソース] の下の [フォールバック ローカル アイデンティティ ソース] フィールドに表示します（認証タイプとして [AAA] を選択すると、この属性が表示されます）。

    CDO で読み取られるサーバーグループ属性の詳細については、「AAA サーバグループ」を参照してください。

セカンダリ アイデンティティ ソース

[セカンダリ アイデンティティ ソース] には、ASA デバイスのセカンダリ認証属性が表示されます。これらの属性を表示するには、認証タイプとして [AAA] または [AAAとクライアント証明書] を選択し、[セカンダリ アイデンティティ ソースの表示] をクリックします。

- [ユーザー認証用セカンダリ アイデンティティ ソース] に、セカンダリ認証の**サーバーグループ**属性が表示されます。
  - **サーバーグループ**が LOCAL 以外に設定されている場合、CDO はこの属性を読み取り、[セカンダリ アイデンティティ ソース] の下の [セカンダリ用フォールバック ローカル アイデンティティ ソース] フィールドに表示します。
- CDOは、**属性サーバー**および**インターフェイス固有の承認サーバーグループ**属性をサポートしていません。

CDO で読み取られるサーバーグループ属性の詳細については、「AAA サーバグループ」を参照してください。

承認サーバー

- [承認サーバー] には承認**サーバーグループ**の属性が表示されます。
- CDO は、インターフェイスとサーバーグループを持つ承認サーバーグループをサポートしていません。

CDO で読み取られる RADIUS サーバーグループ属性の詳細については、「RADIUS サーバグループ」を参照してください。

アカウンティングサーバー

アカウンティングサーバーは、アカウンティング **サーバー グループ**属性を表示します。CDO で読み取られるサーバーグループ属性の詳細については、「RADIUS サーバグループ」を参照してください。

クライアントアドレスプールの割り当て

CDO は、**クライアントアドレス割り当て属性（DHCP サーバー、クライアントアドレスプール、クライアント IPv6 アドレスプール**）をオブジェクトとして読み取ります（これらの属性は「**クライアントアドレスプールの割り当て**」で確認できます）。DHCP サーバーの詳細はリテラルとして読み取られます。

（注） CDO は、特定のインターフェイスに割り当てられた IP アドレスプールをサポートしていません。ただし、これらの属性はASA コマンドライン インターフェイス（CLI）で確認できます。

AAA サーバグループ

CDO は、LDAP サーバーグループとそれに関連付けられた LDAP サーバーを、[Active Directory レルム（Active Directory Realm）] オブジェクトとして表します。Active Directory（AD）の場合、レルムは Active Directory ドメインに相当します。CDO は、既に存在する AD レルムオブジェクトの AD パスワードを読み取ります。

ステップ 1 [オブジェクト] で、[Active Directoryレルム（Active Directory レルム）] フィルタを適用して、このオブジェクトを表示できます。

ステップ 2 必要な Active Directory レルムオブジェクトを選択して、[編集] をクリックして詳細を表示します。

次のタスク

AD レルムには、関連付けられた AD サーバーとその設定が含まれていることがわかります。AD レルムに対して複数の Active Directory（AD）サーバーが存在する場合、AD サーバーは相互に複製されていて、同じ AD ドメインをサポートする必要があります。したがって、ディレクトリ名、ディレクトリパスワード、ベース識別名などの基本的なレルムプロパティは、その AD レルムに関連付けられたすべての AD サーバーで同じである必要があります。これらのプロパティが同じでない場合、CDO は Active Directory レルムオブジェクトに警告メッセージを表示します。これらのプロパティを修正して、AD サーバー全体で一貫性を持たせる必要があります。この警告に対処せずに続行すると、CDO はいずれかの AD サーバープロパティを使用し、そのレルムオブジェクト内の他のサーバーに適用します。

RADIUS サーバグループ

ASA デバイスの AAA RADIUS サーバーグループ属性は、CDO では RADIUS サーバー グループ オブジェクトとして読み取られます。

ステップ 1 [オブジェクト] で RADIUS サーバーグループフィルターを適用して、このオブジェクトを表示できます。

ステップ 2 必要なオブジェクトを選択して、[編集] をクリックして詳細を表示します。

- ASA での [ダイナミック認証の有効化（Enable dynamic authorization）]は、CDO では [ダイナミック認証（RA VPNの場合のみ）（Dynamic Authorization (for RA VPN only)）] として読み取られます。
- [再アクティブ化モード（Reactivation Mode）] の [枯渇（Depletion）] オプションは CDO で読み取られるため、枯渇時間に関連する [デッドタイム値（Dead Time）] も CDO で読み取られます。ただし、[時間指定（Timed）] 属性は CDO で読み取られません。
- CDO は、[アカウンティングモード（Accounting Mode）]、[時間指定（Timed）]、[中間アカウンティングアップデートの有効化（Enable interim accounting update）]、[中間アカウンティングアップデートの有効化（Enable interim accounting update）]、および [認可専用モードの使用（Use authorization only mode）] をサポートしていません。

RADIUS サーバ

CDO が ASA から Radius サーバーを読み取ると、「Radius サーバーグループの名前_サーバー名または IPアドレス」という名前を指定する Radius サーバーオブジェクトが作成されます。

ステップ 1 [オブジェクト] で [RADIUSサーバー（RADIUS Server）] フィルタを適用して、このオブジェクトを表示できます。

ステップ 2 必要なオブジェクトを選択して、[編集（Edit）] をクリックして詳細を表示します。

Group Policy

[グループポリシー（Group Policy）] セクションでドロップダウンをクリックして、デバイスに関連付けられたグループポリシーを表示します。

注目 CDOは、トンネリングプロトコルでSSL VPNクライアントとして設定されたグループポリシーを読み取ります。

CDOは、ASAで設定されたグループポリシー属性の大部分を読み取ります。情報は、RA VPNグループポリシーウィザードの複数のタブにわたって表示されます。ASAデバイスから読み取られたグループポリシーの詳細を表示するには、次を実行する必要があります。

ステップ 1 CDO ナビゲーションバーで、[オブジェクト] をクリックし、[RA VPNグループポリシー（RA VPN Group Policy）] でフィルタリングします。

ステップ 2 そのデバイスに関連付けられているグループポリシーを選択し、[編集] をクリックします。

次のタスク

（注） CDO は、ASA デバイスのスプリットトンネリングで定義されている標準アクセス制御リスト（ACL）をサポートしていません。CDO は拡張アクセス制御リスト（ACL）をサポートし、ASA ポリシーの ACL として読み取ります。詳細については、「ASA RA VPN グループポリシー属性」を参照してください。ポリシーを表示するには、ナビゲーションバーで [ポリシー（Policies）] > [ASAアクセスポリシー（ASA Access Policies）] をクリックします。

拡張 ACL を選択するには、次の手順を実行します。

- [スプリットトンネリング（Split Tunneling）] タブをクリックします。
- ASA のトラフィックが IPv4 または IPv6 アドレスのどちらを使用するかに基づいて、対応するドロップダウンリストから [トンネル経由の指定したトラフィックを許可する（Allow specified traffic over tunnel）] または [以下に指定したネットワークを除外する（Exclude

networks specified below）] を選択します。ASA からインポートされた拡張 ACL を選択します。

IP アドレスプールの作成

ASA の IPv4 および IPv6 IP アドレスプールを設定して、VPN 接続を使用してネットワークにリモート接続しているクライアントにそれらを割り当てることができます。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定すると、ASA は追加された順でそれらのプールを使用します。

IPv4 アドレスプールを定義するには、IP アドレス範囲を指定します。IPv4 アドレスプールの例は、10.10.147.100 - 10.10.147.177 です。

IPv6 アドレスプールを設定するには、開始 IP アドレス範囲、アドレスプレフィックス、プールに設定できるアドレス数を指定します。IPv6 アドレスプールの例は、2001:DB8:1::1 です。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

IP アドレスプールを作成するには、次の手順を実行します。

ステップ 1 CDO ナビゲーションバーで [オブジェクト（Objects）] をクリックして、[オブジェクト（Objects）] ページを表示します。

ステップ 2 青いプラスボタン  をクリックし、**[ASA] > [アドレスプール]**を選択します。

ステップ 3 [IPアドレスプールの作成（Create IP Address Pool）] ダイアログボックスで、次の情報を入力します。

- [オブジェクト名] : 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。
- [IPv4アドレスプール] : このラジオボタンを選択して、IPv4 アドレスプールを設定します。
  - [IPv4アドレス範囲（IPv4 Address Range）] : 設定された各プールで使用可能な最初の IP アドレスと最後の IP アドレスを入力します。たとえば、10.10.147.100 - 10.10.147.177 です。
  - [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。
- [IPv6アドレスプール] : このラジオボタンを選択して、IPv4 アドレスプールを設定します。
  - [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、 <address>/<prefix> 形式で入力します。たとえば、2001:DB8:1::1/3 です。
  - [アドレスの数（Number of Addresses）] : 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。

ステップ 4 [保存（Save）] をクリックします。

リモートアクセス VPN 認証ベースの認証

リモートアクセス VPN は、次のシナリオでセキュアゲートウェイおよび AnyConnect クライアント（エンドポイント）を認証するためにデジタル証明書を使用します。

重要 CDO は、VPN ヘッドエンド（ASA ）へのデジタル証明書のインストールを処理します。AnyConnect クライアントデバイスへの証明書のインストールは処理されません。これは、組織の管理者が処理する必要があります。

- VPN ヘッドエンドデバイス（ASA ）を識別して認証します。

  VPN ヘッドエンドは、AnyConnect クライアントが VPN 接続を要求するときに、VPN ヘッドエンド自体を識別して認証するための ID 証明書を必要とします。CDO を使用して、デバイスに ID 証明書をインストールする必要があります。「PKCS12 を使用した ID 証明書をインストールする」または「証明書とキー」を参照してください。AnyConnect クライアントに発行元の CA 証明書をインストールすることは、必須ではありません。

  CDO からリモートアクセス VPN 構成を作成するときに、登録済み ID 証明書をデバイスの外部インターフェイスに割り当て、構成をデバイスにダウンロードします。ID 証明書は、デバイスの外部インターフェイスで完全に機能するようになります。

  AnyConnect クライアントが VPN への接続を試みると、デバイスは、その ID 証明書を AnyConnect クライアントに提示することにより、それ自体を認証します。AnyConnect クライアントは、信頼できる CA 証明書を使用してこの ID 証明書を検証し、その証明書を信頼することによってデバイスを信頼します。AnyConnect クライアントに CA 証明書がインストールされていない場合、プロンプトが表示されたときに、ユーザーがデバイスを手動で信頼する必要があります。

- AnyConnect クライアントを識別して認証します。

  （注） これは、RA VPN 構成の接続プロファイルで認証方式として「クライアント証明書のみ」または「AAA とクライアント証明書」を使用する場合に適用されます。「AAA のみ」には適用されません。

  デバイスが信頼されると、AnyConnect クライアントは、VPN 接続を完了するためにそれ自体を認証する必要があります。AnyConnect クライアントに ID 証明書をインストールし、CDO を使用して、信頼できる CA 証明書をデバイスにインストールする必要があります。これらの証明書は、同じ認証局によって発行される必要があります。「ASA の信頼できる証明書をインストールする」を参照してください。

  AnyConnect クライアントが ID 証明書を提示し、デバイスは、この証明書を信頼できる CA 証明書で検証して、VPN 接続を確立します。

NAT からの ASA リモート アクセス トラフィックの除外

リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を設定します。VPN トラフィックを NAT 免除にしない場合は、外部および内部インターフェイスに対する既存の NAT ルールが RA VPN アドレス プールに適用されないことを確認してください。NAT 免除 ルールは特定の送信元/宛先インターフェイスとネットワークの組み合わせに対する手動スタティック アイデンティティ NAT ルールですが、NAT ポリシーには反映されず、非表示になります。NAT 免除を有効にした場合、以下も設定する必要があります。

- [内部インターフェイス（Inside Interfaces）]：リモートユーザーがアクセスする内部ネットワークのインターフェイスを選択します。これらのインターフェイスには NAT ルールが作成されます。
- [内部ネットワーク（Inside Networks）]：リモートユーザーがアクセスする内部ネットワークを表すネットワークオブジェクトを選択します。ネットワークリストには、サポートしているアドレス プールと同じ IP タイプを含める必要があります。

始める前に

デバイスの接続プロファイルおよびグループポリシーで使用されるローカル IP アドレスプールの設定に一致する ASA ネットワークオブジェクトを作成します。それらのネットワークオブジェクトは、NAT ルールを設定するときに、宛先アドレスおよび変換されたアドレスとして割り当てる必要があります。「ASA ネットワークオブジェクトの作成 （13 ページ）」を参照してください。

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイスとサービス] フィルタと [検索] フィールドを使用して、NAT ルールを作成する ASA デバイスを見つけます。

ステップ 3 詳細パネルの [管理] 領域で、[NAT] NAT をクリックします。

ステップ 4 + > [Twice NAT] をクリックします。

1. セクション 1 で、[静的（Static）] を選択します。 [続行（Continue）] をクリックします。
2. セクション 2 で、[送信元インターフェイス（Source Interface）] で [any] および [宛先インターフェイス（Destination Interface）] で [any] を選択します。[続行] をクリックします。
3. セクション 3 で、[送信元の元のアドレス（Source Original Address）] で [any] および [送信元の変換後アドレス（Source Translated Address）] で [any] を選択します。
4. [宛先を使用（Use Destination）] を選択します。
    1. [宛先の元のアドレス（Destination Original Address）] と [送信元の変換後アドレス（Source Translated Address）]：ドロップダウンで [選択（Choose）] をクリックし、ローカル IP アドレスプールの設定に一致するネットワークオブジェクトを選択します。次の例では、「IPV4_Object」は、ASA（BGL_ASA1_SH）デバイスの接続プロファイルおよびグループポリシー設定で使用される IPv4

アドレスプールオブジェクトと同じ設定を持つネットワークオブジェクトです。

2. [着信パケットのプロキシARPの無効化（Disable proxy ARP for incoming packets）] を選択します。
3. [保存（Save）] をクリックします。
4. プロセス（ステップ 4 から）を繰り返して、IP アドレスプールに相当する他のネットワークオブジェクトごとに同等のルールを作成します。

ステップ 5 CDO から ASA に設定変更を展開します。。

ユーザーが AnyConnect クライアントソフトウェアを ASA にインストールする方法

VPN 接続を完了するには、ユーザは AnyConnect クライアント ソフトウェアをインストールする必要があります。既存のソフトウェア配布方式を使用して、ソフトウェアを直接インストールできます。または、ASA デバイスから AnyConnect クライアントを直接インストールすることもできます。

（注） ソフトウェアをインストールするには、ユーザにワークステーションでの管理者権限が必要です。

ソフトウェアの最初のインストールを ASA デバイスからユーザーに行ってもらう場合、以下の手順を実行するようにユーザーに指示します。

（注） Android および iOS のユーザは、適切な App Store から AnyConnect をダウンロードする必要があります。

ステップ 1 Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。このインターフェイスは、リモート アクセス VPN を設定する際に指定します。ログインを指示するメッセージがユーザに示されます。

ステップ 2 サイトにログインします。ユーザは、リモート アクセス VPN 用に設定されたディレクトリ サーバを使用して認証されます。続行するには、ログインが正常に行われる必要があります。ログインが成功すると、システムは、必要となる AnyConnect クライアントのバージョンがインストールされているかを確認します。AnyConnect クライアントがユーザーのコンピュータにないか、下位のバージョンである場合、システムは自動的に AnyConnect ソフトウェアのインストールを開始します。インストールが終了すると、AnyConnect がリモートアクセス VPN 接続を完了します。

導入準備済み ASA のリモートアクセス VPN 設定の変更

ASA デバイスが CDO に導入準備されると、導入準備された ASA デバイスから既存のリモートアクセス VPN 設定を検出して表示します。詳細については、オンボーディング済み ASA デバイスの RA VPN 設定の読み取り （120 ページ）を参照してください。

これらの設定を変更して、新しい設定をデバイスにダウンロードできます。

- ASA RA VPN 構成の変更
- ASA 接続プロファイルの変更

リモートアクセス *VPN* 設定の変更

ステップ 1 左側の CDO ナビゲーションバーで、[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。

ステップ 2 グループポリシーを VPN 設定に追加または削除する場合は、導入準備の ASA デバイスに関連付けられている VPN 設定をクリックします。左側の [操作（Actions）] ウィンドウで、[グループポリシー（Group Policies）] をクリックします。

a) 青い [+] アイコンをクリックして選択を設定し、[選択（Select）] をクリックします。
b) [保存（Save）] をクリックします。新しい新規 ASA RA VPN グループポリシーの作成を作成することもできます。

ステップ 3 [VPN設定（VPN configuration）] をクリックし、左側の [操作（Actions）] ウィンドウで [編集] をクリックします。

ウィザードには、設定に関連付けられている ASA デバイスが一覧表示されます。

a) 作成時と同じ方法で、次の詳細を変更できます。

- RA VPN 設定の名前を変更します。
- デバイスの詳細が表示されている行に表示される 3 つのドットをクリックし、[編集] をクリックします。

詳細については、ASA RA VPN 設定の作成 （105 ページ）を参照してください。

ステップ 4 [OK] をクリックします。

ステップ 5 すべてのデバイスの構成変更のプレビューと展開 （178 ページ）

ASA 接続プロファイルの変更

ステップ 1 左側の CDO ナビゲーションバーで、[VPN] > [リモートアクセスVPNの設定（Remote Access VPN Configuration）] をクリックします。

ステップ 2 導入準備の ASA デバイスに関連付けられている VPN 設定を展開し、接続プロファイルを選択します。

ステップ 3 左側の [アクション] ペインで、[編集] をクリックします。

ステップ 4 作成時と同じ方法で値を編集し、[完了（Done）] をクリックします。

詳細については、「ASA RA VPN 接続プロファイルの設定 （109 ページ）」を参照してください。

ステップ 5 すべてのデバイスの構成変更のプレビューと展開 （178 ページ）

RA VPN AnyConnect クライアントプロファイルのアップロード

リモートアクセス VPN AnyConnect クライアントプロファイルは、ファイルに保存されている設定パラメータのグループです。AnyConnect クライアントプロファイルにはさまざまな種類があり、コアクライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、AMP イネーブラ、ISE ポスチャ、ネットワークの可視性、カスタマー フィードバック エクスペリエンス プロファイル、Umbrella ローミングセキュリティ、Web セキュリティの構成設定が含まれています。

CDO では、後でグループポリシーで使用できるオブジェクトとしてこれらのプロファイルをアップロードできます。

- [AnyConnect VPNプロファイル（AnyConnect VPN Profile）]：AnyConnect クライアントプロファイルは、VPN AnyConnect クライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーが AnyConnect クライアントの設定および詳細設定からオプションを変更できるかどうかを定義します。CDO は XML ファイル形式をサポートしています。
- [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 AnyConnect 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 イネーブラがこのプロファイルと共に FTD からエンドポイントにプッシュされます。CDO は、XML および ASP ファイル形式をサポートしています。
- [フィードバックプロファイル（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。CDO は FSP ファイル形式をサポートしています。

- [ISEポスチャプロファイル（ISE Posture Profile）]：AnyConnect 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。CDO は、XML および ISP ファイル形式をサポートしています。
- [ネットワークアクセスマネージャサービスプロファイル（Network Access Manager 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。CDO は、XML および NSP ファイル形式をサポートしています。
- [ネットワーク可視性サービスプロファイル（Network Visibility Service Profile）]：AnyConnect 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。CDO は、XML および NVMSP ファイル形式をサポートしています。
- [Umbrellaローミングセキュリティプロファイル（Umbrella Roaming Security Profile）]：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。CDO は、XML および JSON ファイル形式をサポートしています。
- [Webセキュリティサービスプロファイル（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。CDO は、XML、WSO、および WSP ファイル形式をサポートします。

始める前に

適切な GUI ベースの AnyConnect プロファイルエディタを使用して、必要なプロファイルを作成します。AnyConnect セキュア モビリティ クライアント カテゴリの Cisco Software Download Center からプロファイルエディタをダウンロードし、AnyConnect の「プロファイルエディタ - Windows/スタンドアロンインストーラ（MSI）」をインストールできます。プロファイルエディタのインストーラには、スタンドアロンバージョンのプロファイルエディタが含まれています。このインストールファイルは Windows 専用で、ファイル名は anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> は AnyConnect のバージョンです。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイル エディタをインストールする前に、Java JRE（1.6 以降）もインストールする必要があります。

このパッケージには、Umbrella ローミング セキュリティ プロファイル エディタを除き、モジュールの作成に必要なすべてのプロファイルエディタが含まれています。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「*AnyConnect* プロファイルエディタ」の章を参照してください。Umbrella ダッシュボードから Umbrella ローミング セキュリティ プロファイルを個別にダウンロードします。詳細については、『Cisco Umbrella User Guide』の「Umbrella ローミングセキュリティ」章の「Umbrella ダッシュボードから AnyConnect ローミング セキュリティ プロファイルをダウンロードする」セクションを参照してください。

ステップ 1 左側の CDO ナビゲーションバーで、[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ます。

ステップ 3 **[RA VPNオブジェクト（ASA & FTD）（RA VPN Objects (ASA & FTD)）] > [AnyConnectクライアントプロファイル（AnyConnect Client Profile）]**をクリックします。

ステップ 4 [オブジェクト名] フィールドに、AnyConnect クライアントプロファイルの名前を入力します。

ステップ 5 [参照] をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 6 [開く（Open）] をクリックしてプロファイルをアップロードします。

ステップ 7 [追加] をクリックしてオブジェクトを追加します。

関連情報：

- RA VPN グループポリシーウィンドウで、クライアントモジュールを AnyConnect VPN プロファイルに関連付けます。「新規 ASA RA VPN グループポリシーの作成」を参照してください。

（注） クライアントモジュールの関連付けは、すべての ASA バージョン、およびソフトウェアバージョン 6.7 以降を実行している FTD でサポートされています。

ASA のリモートアクセス VPN 設定の確認

リモートアクセス VPN を設定し、設定をデバイスに展開した後で、リモート接続できることを確認します。

ステップ 1 外部ネットワークから、AnyConnect クライアントを使用して VPN 接続を確立します。Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。必要に応じて、クライアントソフトウェアをインストールし、接続を完了します。「ユーザーが AnyConnect クライアントソフトウェアを ASA にインストールする方法」を参照してください。グループ URL を設定した場合は、グループ URL も試してください。

ステップ 2 [デバイスとサービス] ページで、確認するデバイス（FTD または ASA）を選択し、[デバイスアクション] の下の [コマンドラインインターフェイス（Command Line Interface）] をクリックします。

ステップ 3 **show vpn-sessiondb** コマンドを使用して、現在の VPN セッションに関する概要情報を表示します。

ステップ 4 統計情報では、アクティブな AnyConnect クライアント セッション、および累積セッション数、ピーク同時セッション数、非アクティブ セッション数の情報が示されます。次は、コマンドからの出力例です。

```
> show vpn-sessiondb
--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------


  Total Active and Inactive    :      1             Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  --------------------------------------------------------------------------

  --------------------------------------------------------------------------
  Tunnels Summary
  --------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
  Clientless                 :      0 :          1 :               1
  AnyConnect-Parent          :      1 :         49 :               3
  SSL-Tunnel                 :      1 :         46 :               3
  DTLS-Tunnel                :      1 :         46 :               3
  --------------------------------------------------------------------------
  Totals                     :      3 :        142
  --------------------------------------------------------------------------

  --------------------------------------------------------------------------
  IPv6 Usage Summary
  --------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
  AnyConnect SSL/TLS/DTLS    :        :           :
    Tunneled IPv6            :      1 :         20 :           2
  --------------------------------------------------------------------------
```

ステップ 5 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の AnyConnect VPN セッションに関する詳細情報を表示します。詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含まれます。VPN 接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

ステップ 6 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の AnyConnect VPN セッションに関する詳細情報を表示します。詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含

まれます。VPN 接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

ASA のリモートアクセス VPN 設定の詳細表示

ステップ 1 左側の CDO ナビゲーションバーで、**[VPN]** > **[リモートアクセスVPNの設定（Remote Access VPN Configuration）]**をクリックします。

ステップ 2 表示された VPN 設定オブジェクトをクリックします。グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

- RA VPN 設定を展開して、それらに関連付けられているすべての接続プロファイルを表示します。
  - 追加 + ボタンをクリックして新しい接続プロファイルを追加します。
  - 表示ボタン（  ）をクリックして、接続プロファイルの概要と接続手順を開きます。[アクション（Actions）] で、[編集（Edit）] をクリックして変更を変更できます。
- [アクション（Actions）] で次のオプションのいずれかをクリックすると、追加のタスクを実行できます。
  - グループポリシーを割り当て/追加するには、[グループポリシー（Group Policies）] をクリックします。
  - 不要になった設定オブジェクトまたは接続プロファイルをクリックし、[削除（Remove）] をクリックして削除します。

ASA のテンプレート

テンプレートを使用すると、汎用のデバイス/サービス構成を構築できるため、その構成をグループ化された他の構成に適用できます。これらのテンプレートにより、グループ化された多くの実装に影響を与えるための変更を一箇所で行うことができます。

ASA テンプレートパラメータ

新しいテンプレートを作成する際、特定のデバイスをモデルにしたいことがあります。CDO には、テンプレートがモデル化されたデバイスの設定内にあるテキストの選択されたフィールドに基づいてテンプレートパラメータを設定する機能があります。パラメータは、作成するか、既存のパラメータから設定する、またはテンプレート パラメータ ビュー内で検索することができます。

（注） ASAテンプレートの設定をインポートすることを選択した場合、設定はJSON形式である必要があります。

新規パラメータの作成

ステップ 1 既存のデバイスが導入準備された状態で、CDO の上部にある [テンプレート] タブに移動します。
ステップ 2 [新しいテンプレート（New Template）] または [テンプレートの管理（Manage Templates）] を選択します。
ステップ 3 必要な設定を選択してパラメータを作成します。
ステップ 4 画面上部にある [名前（Name）] フィールドに入力することによってテンプレートに名前を付けます。
ステップ 5 パラメータを追加する目的のテキストフィールドを選択します。
ステップ 6 パラメータに説明を付け、値と必要な注記を追加します。
ステップ 7 [名前（Name）] フィールドの横にある [保存（Save）] をクリックしてパラメータを保存します。
ステップ 8 その後、[テンプレートの確認（Review Template）] をクリックして、テンプレートを確認することができます。

これで、今後このテンプレートを使用して導入準備されるすべてのデバイスに適用されるパラメータが作成され、保存されました。

新規 ASA、ISR、ASR テンプレートの作成

基本設定

既知のASA、ISR、またはASRの基本設定から始めます。目的の設定を選択して、テンプレートのパラメータ化を開始します。パラメータ化には、構成ファイル内のフィールドまたは属性の選択と、構成ファイルのインスタンス化で選択される値のリストの識別が含まれます。

（注） ASAテンプレートの設定をインポートすることを選択した場合、設定はJSON形式である必要があります。

パラメータの追加

基本設定を選択すると、パラメータ化プロセスを開始できます。設定エディタから、パラメータ化する目的のフィールドを選択します。選択した文字列は二重括弧で囲まれています。左ペインから、パラメータの名前を変更したり、説明を追加したり、複数の値を追加したりできます。[カスタム値を許可（Allow Custom Value）] を選択すると、インスタンス化時にカスタム値を設定できます。それ以外の場合は、識別された値のみ選択できます。

パラメータ化が完了したら、テンプレートの名前を指定し、[保存（Save）] をクリックします。

パラメータ化の詳細については、ASA テンプレートパラメータを参照してください。

レビュー

テンプレートを保存したら、[レビュー（Review）] をクリックしてレビュープロセスに移動します。レビューでは、パラメータ化された値を含め、テンプレートをそのままエクスポートできます。これは必ずしも有効な設定ではありませんが、CDO に保存されているテンプレートを確認する手段が提供されます。必要に応じて、[編集] をクリックしてテンプレートを編集することもできます。[差分（Diff）] ボタンを使用すると、保存されたテンプレートと最新の編集との違いが表示されます。

テンプレートからの ASA 設定の生成

テンプレートからの設定の作成

テンプレートからカスタム設定を生成するプロセスを開始するには、[テンプレートから設定（Config from Template）] ボタンをします。使用可能なテンプレートが一覧表示されます。該当するテンプレートを選択して、[テンプレートの選択（Choose Template）] をクリックします。

ほとんどの場合、テンプレートには、設定をカスタマイズするために [エクスポート（Export）] で設定する必要があるパラメータ化された値が含まれます。左側のペインから、この設定に必要な各パラメータと値を選択します。値がエディターに示されるので注目してください。これらは、エクスポート時にパラメータを置き換える値です。すべてのパラメータ値を設定したら、[エクスポート（Export）] ボタンをクリックして設定をエクスポートし、ダウンロードします。テンプレートにパラメータ化された値が含まれていない場合は、[エクスポート（Export）] ボタンをクリックして設定をそのままエクスポートします。

ASA テンプレートの管理

[テンプレートの管理（Manage Templates）] ビューでは、既存のすべてのテンプレートを可視化し、それらを編集および削除することができます。パラメータ化と値の構成は、テンプレートの編集中に変更できます。その方法は、既存のテンプレートにマウスのカーソルを合わせて、[編集] を選択して変更を加えるだけです。

テンプレートの編集

編集ビューでは、次の作業を実行できます。

- エディタのテキストをダブルクリックまたは強調表示して、パラメータを追加します。
- 説明のテキストボックスに入力して、パラメータを説明します。その後に、[値の追加（Add Value）] をクリックします。
- 値を指定し、注記を入力します。[追加（Add）] をクリックします。
- 完了したら、[Save] をクリックします。
- ここで、[テンプレートの確認（Review Template）] をクリックして、テンプレートを確認することができます。
  - [差分（Diff）] をクリックして、ファイルを比較することができます。
  - テンプレートをエクスポートするには、[Export（エクスポート）] をクリックします。

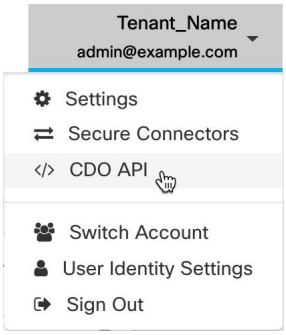
CDO パブリック API

CDO はパブリック API を公開しており、ドキュメント、例、試してみるためのプレイグラウンドを提供しています。パブリック API の目標は、通常は CDO UI で実行できる多くのことをコードで実行するためのシンプルで効果的な方法を提供することです。

この API を使用するには、GraphQL の知識が必要です。詳細でありながら読みやすい公式ガイド（https://graphql.org/learn/）が提供されています。

完全なスキーマドキュメントを見つけるには、GraphQL Playground に移動し、ページの右側にある [ドキュメント（docs）] タブをクリックしてください。

ユーザーメニューから選択して、CDO パブリック API を起動できます。



API トークン

開発者は、CDO REST API 呼び出しを行うときに CDO API トークンを使用します。呼び出しを成功させるには、API トークンを REST API 認証ヘッダーに挿入する必要があります。API

トークンは、有効期限のない「長期的な」アクセストークンですが、更新したり、取り消したりできます。

CDO 内から API トークンを生成できます。生成されたトークンは、生成直後に、[一般設定（General Settings）] ページが開いている間のみ表示されます。CDO で別のページを開いてから [一般設定（General Settings）] ページに戻ると、トークンが発行されたことはわかりますが、トークンは表示されなくなります。

個々のユーザーは、特定のテナントに対して独自のトークンを作成できます。あるユーザーが別のユーザーに代わってトークンを生成することはできません。トークンはアカウントとテナントのペアに固有であり、他のユーザーとテナントの組み合わせには使用できません。

API トークン形式とクレーム

API トークンは JSON Web トークン（JWT）です。JWT トークン形式の詳細については、「Introduction to JSON Web Tokens」を参照してください。

CDO API トークンは、次の一連のクレームを提供します。

- **id**：ユーザー/デバイス uid
- **parentId**：テナント uid
- **ver**：公開キーのバージョン（初期バージョンは 0、例：**cdo_jwt_sig_pub_key.0**）
- **subscriptions**：SSE サブスクリプション（任意）
- **client_id**：「**api-client**」
- **jti**：トークン id

ASA 証明書の管理

デジタル証明書は、デバイスや個々のユーザーの認証に使用されるデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザーまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザーまたはデバイスの公開キーのコピーも含まれています。デジタル証明書の詳細については、『Cisco ASA Series General Operations ASDM Configuration, X.Y』ドキュメントの「Basic Settings」ブックの「Digital Certificates」の章を参照してください。

認証局（CA）は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザーのアイデンティティを保証する、信頼できる機関です。CA はID 証明書も発行します。

- **ID 証明書**：ID 証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。CA は、特定のシステムまたはホストの証明書である ID 証明書を発行します。
- **信頼できる認証局（CA）証明書**：信頼できる CA 証明書は、システムで他の証明書への署名に使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内

部アイデンティティ証明書と異なります。これらはCA 証明書では有効ですが、アイデンティティ証明書では無効です。信頼できる CA 証明書は自己署名され、ルート証明書と呼ばれます。

リモートアクセス VPN は、セキュリティで保護された VPN 接続を確立するために、セキュアゲートウェイおよび AnyConnect クライアント（エンドポイント）を認証するためのデジタル証明書を使用します。詳細については、「リモートアクセス VPN 認証ベースの認証」を参照してください。

証明書のインストールに関するガイドライン

ASA での証明書のインストールに関する以下のガイドラインをお読みください。

- 証明書は、1 つの ASA デバイスに、または複数の ASA デバイスに同時にインストールできます。
- 証明書は一度に 1 つだけインストールできます。
- 証明書は、ライブ ASA デバイスにのみインストールできます。モーダルデバイスにはインストールできません。
- 証明書は、 Secure Firewall Cloud Native デバイスにインストールできません。

ASA 証明書のインストール

デジタル証明書をトラストポイントのオブジェクトとしてアップロードし、CDO によって管理される ASA デバイスにインストールする必要があります。

（注） ASAデバイスにアウトオブバンドの変更がなく、ステージングされたすべての変更が展開されていることを確認します。

CDO でサポートされているデジタル証明書と形式を次に示します。

- ID 証明書は、次の方法を使用してインストールできます。
  - PKCS12 ファイルのインポート。
  - 自己署名証明書。
  - 証明書署名要求（CSR）のインポート。
- 信頼できる CA 証明書は、PEM または DER 形式を使用してインストールできます。

CDO を使用して ASA に証明書をインストールする手順を示すスクリーンキャストをご覧ください。インストールされている証明書を変更、エクスポート、および削除する手順も示しています。

サポートされている証明書形式

- PKCS12：PKCS#12、P12、または PFX 形式は、サーバー証明書、あらゆる中間証明書、および秘密キーを 1 つの暗号化可能ファイルに格納するためのバイナリ形式です。PFX ファイルには通常、**.pfx** や **.p12** などの拡張子が付いています。
- PEM：PEM（元は「Privacy Enhanced Mail」）ファイルには ASCII（または Base64）エンコードデータが含まれており、証明書ファイルは .pem、.crt、.cer、または .key 形式にすることができます。これらは Base64 でエンコードされた ASCII ファイルで、「-----BEGIN CERTIFICATE-----」および「-----END CERTIFICATE-----」ステートメントが含まれています。
- DER：DER（Distinguished Encoding Rule）形式は、ASCII PEM 形式ではなく、シンプルなバイナリ形式の証明書です。**.der** ファイル拡張子が付いている場合もありますが、**.cer** ファイル拡張子が付いていることが多いため、DER の.cer ファイルと PEM の .cer ファイルを区別する唯一の方法は、テキストエディタで開いて、 BEGIN/END ステートメントの有無を確認することです。PEM とは異なり、DER でエンコードされたファイルには、 -----BEGIN CERTIFICATE----- などのプレーン テキスト ステートメントは含まれません。

トラストポイント画面

ASA デバイスを CDO に導入準備した後、[デバイスとサービス] タブで ASA デバイスを選択し、左側の [管理] ペインで [トラストポイント] をクリックします。

[トラストポイント] タブに、デバイスにインストール済みの証明書が表示されます。

- [インストール済み（Installed）] ステータスは、対応する証明書がデバイスに正常にインストールされたことを示します。
- 「不明（Unknown）」ステータスは、対応する証明書に情報がなにも含まれていないことを示します。このような証明書は削除して、正しい情報を含む証明書を再度アップロードする必要があります。CDO は、すべての不明な証明書を信頼できる CA 証明書として検出します。
- [インストール済み（Installed）] と表示されている行をクリックして、右側のペインに証明書の詳細を表示します。[詳細（More）] をクリックして、選択した証明書の詳細を表示します。
- インストールされたID 証明書は、PKCS12 または PEM 形式でエクスポートして、他の ASA デバイスにインポートできます。「ID 証明書のエクスポート」を参照してください。
- インストールされた証明書で変更できるのは、詳細設定のみです。
  - [編集] をクリックして、詳細設定を変更します。
  - 変更を加えたら、[送信（Send）] をクリックして、更新された証明書をインストールします。

PKCS12 を使用した ID 証明書のインストール

PKCS12 形式用に作成された既存のトラストポイント オブジェクトを選択して、ASA デバイスにインストールできます。インストールウィザードから新しいトラストポイント オブジェクトを作成し、ASA デバイスに証明書をインストールすることもできます。

始める前に

- 「証明書のインストールに関するガイドライン」を読みます。
- ASA は [同期（Synced）] 状態で [オンライン] である必要があります。

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 単一の ASA デバイスに ID 証明書をインストールするには、次の手順を実行します。

a) [デバイス] タブをクリックします。
b) [ASA] タブをクリックして、ASA デバイスを選択します。
c) 右側の [管理] ペインで、[トラストポイント] をクリックします。
d) [Install（インストール）] をクリックします。

（注） 複数の ASA デバイスに証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション（Devices Action）] で [証明書のインストール（Install Certificate）] をクリックします。

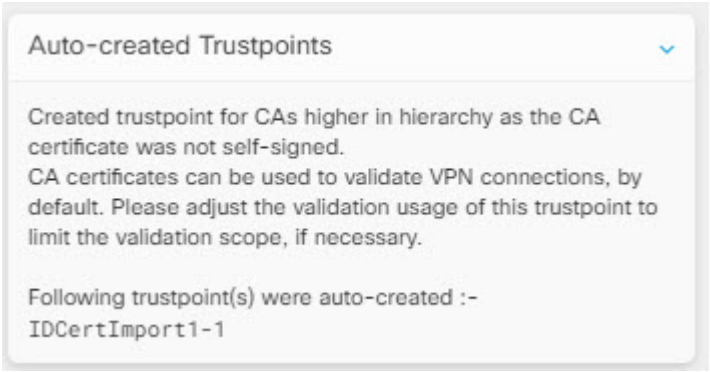
ステップ 3 [インストールするトラストポイント証明書の選択（Select Trustpoint Certificate to Install）] で、次のいずれかをクリックします。

- [作成（Create）]：新しいトラストポイント オブジェクトを追加します。詳細については、「PKCS12 を使用したID 証明書オブジェクトを追加する」を参照してください。
- [選択（Choose）]：PKCS タイプの証明書登録オブジェクトを選択します。

ステップ 4 [送信（Send）] をクリックします。

ASA デバイスに証明書がインストールされます。

（注） 中間CAがインストールされているASAにPKCS12証明書をインポートする場合、まだインストールされていないすべての中間 CA 証明書について、トラストポイント オブジェクトが自動的に作成されてデバイスにインストールされます。ID 証明書をクリックすると、次の例のようなメッセージが右側のペインに表示されます。



自己署名登録を使用した証明書のインストール

自己署名証明書用に作成された既存のトラストポイント オブジェクトを選択して、ASA デバイスにインストールできます。インストールウィザードから新しいトラストポイントオブジェクトを作成し、ASA デバイスに証明書をインストールすることもできます。

始める前に

- 証明書のインストールに関するガイドラインを読みます。
- ASA は「同期」状態で「オンライン」である必要があります。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 単一の ASA デバイスに ID 証明書をインストールするには、次の手順を実行します。

a) [デバイス] タブをクリックします。
b) [ASA] タブをクリックして、ASA デバイスを選択します。
c) 右側の [管理（Management）] ペインで、[トラストポイント（Trustpoints）] をクリックします。
d) [Install（インストール）] をクリックします。

（注） 複数の ASA デバイスに署名付き証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション（Devices Action）] で [証明書のインストール（Install Certificate）] をクリックします。

ステップ 3 [インストールするトラストポイント証明書の選択（Select Trustpoint Certificate to Install）] で、次のいずれかをクリックします。

- [作成（Create）]：新しいトラストポイント オブジェクトを追加します。詳細については、「PKCS12 を使用したID 証明書オブジェクトを追加する」を参照してください。
- [選択（Choose）]：自己署名タイプの証明書登録オブジェクトを選択します。

ステップ 4 [送信（Send）] をクリックします。

自己署名登録タイプのトラストポイントの場合は、[発行元の共通名（Issuer Common Name ）] ステータスが常に ASA デバイスとなります。これは、管理対象デバイス自体が独自の CA として機能し、独自のID 証明書を生成するために CA 証明書を必要としないためです。

証明書署名要求（CSR）の管理

最初に CSR リクエストを生成し、信頼できる認証局（CA）によって署名されたこのリクエストを取得する必要があります。次に、CA によって発行された署名付き ID 証明書を ASA デバイスにインストールできます。

- 証明書のインストールに関するガイドラインを読みます。
- ASA は「同期」状態で「オンライン」である必要があります。

次の図は、CSR を生成し、認証された発行済み証明書を ASA にインストールするワークフローを示しています。

CSR リクエストの生成

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 単一の ASA デバイスに ID 証明書をインストールするには、次の手順を実行します。

ステップ 5 [Install（インストール）] をクリックします。

ステップ 6 [インストールするトラストポイント証明書の選択（Select Trustpoint Certificate to Install）] で、次のいずれかをクリックします。

- [作成（Create）]：新しいトラストポイント CSR オブジェクトを追加します。詳細については、証明書署名要求（CSR）用 ID 証明書オブジェクトを追加する （23 ページ）を参照してください。
- [選択（Choose）]：作成済みの CSR リクエストトラストポイントを選択します。

ステップ 7 [送信（Send）] をクリックします。

未署名の証明書署名要求（CSR）が生成されます。

ステップ 8 コピーアイコン copy_icon.png をクリックして、CSR の詳細をコピーします。CSR リクエストは「.csr」ファイル形式でもダウンロードできます。

ステップ 9 [OK] をクリックします。

ステップ 10 証明書に署名するために、証明書署名要求（CSR）を認証局に送信します。

認証局によって発行された署名済みID 証明書のインストール

CA が署名付き証明書を発行したら、それを ASA デバイスにインストールします。

ステップ 1 [トラストポイント（Trustpoint ）] 画面で、[ステータス（Status）] が [署名付き証明書のインストールを待機中（Awaiting Signed Certificate Install）] の CSR 要求をクリックし、右側の [アクション（Actions）] ペインで [認証済みID証明書のインストール（Install Certified ID Certificate）] をクリックします。

ステップ 2 CAから受信した署名付き証明書をアップロードします。ファイルをドラッグアンドドロップするか、その内容を所定のフィールドに貼り付けることができます。トラストポイントコマンドは、選択したトラストポイントに基づいて生成されます。

ステップ 3 [送信（Send）] をクリックします。

これにより、署名付きID証明書がASAデバイスにインストールされます。証明書をインストールすると、変更がすぐにデバイスに展開されます。

（注） 複数の ASA デバイスに証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション（Devices Action）] で [証明書のインストール（Install Certificate）] をクリックします。

ASA の信頼できる証明書をインストールする

始める前に

- 証明書のインストールに関するガイドラインを読みます。
- ASA は「同期済み」状態で「オンライン」である必要があります。

ステップ 1 ナビゲーションメニューで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 単一の ASA デバイスにID 証明書をインストールするには、次の手順を実行します。

a) ASA デバイスを選択し、右側の [管理] ペインで [トラストポイント] をクリックします。

b) [Install（インストール）] をクリックします。

（注） 複数の ASA デバイスに証明書をインストールすることもできます。複数の ASA デバイスを選択し、右側の [デバイスアクション] で [証明書のインストール] をクリックします。

ステップ 5 [インストールするトラストポイント証明書の選択] で、次のいずれかをクリックします。

- [作成]：新しいトラストポイント オブジェクトを追加します。詳細については、信頼できる CA 証明書オブジェクトを追加する （26 ページ）を参照してください。
- [選択] ：信頼された証明機関オブジェクトを選択します。

ステップ 6 [送信（Send）] をクリックします。

これにより、信頼できる CA ファイルが ASA デバイスにインストールされます。

ID 証明書のエクスポート

キーペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式または PEM 形式でエクスポートおよびインポートできます。この形式は、異なる ASA 上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

手順の概要

1. ナビゲーションメニューで、[デバイスとサービス（Devices & Services）] をクリックします。
2. [デバイス] タブをクリックします。
3. [ASA] をクリックします。
4. ASA デバイスを選択し、右側の [管理] で [トラストポイント] をクリックします。
5. ID 証明書をクリックして証明書コンフィギュレーションをエクスポートします。または、検索フィールドに名前を入力することにより、証明書を検索することもできます。
6. 右側の [操作（Actions）] ペインで [証明書のエクスポート（Export Certificate）] をクリックします。
7. [PKCS12 形式（PKCS12 Format）] または [PEM 形式（PEM Format）] をクリックすることにより、証明書の形式を選択します。
8. PKCS12 ファイルをエクスポート用に暗号化するために使用する暗号化パスフレーズを入力します。
9. 暗号化パスフレーズを確認のために再入力します。
10. [エクスポート（Export）] をクリックして、証明書コンフィギュレーションをエクスポートします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ナビゲーションメニューで、[デバイスとサービス（Devices & Services）] をクリックします。	
ステップ 2	[デバイス] タブをクリックします。	
ステップ 3	[ASA] をクリックします。	
ステップ 4	ASA デバイスを選択し、右側の [管理] で [トラストポイント] をクリックします。	
ステップ 5	ID 証明書をクリックして証明書コンフィギュレーションをエクスポートします。または、検索フィールドに名前を入力することにより、証明書を検索することもできます。	
ステップ 6	右側の [操作（Actions）] ペインで [証明書のエクスポート（Export Certificate）] をクリックします。	
ステップ 7	[PKCS12 形式（PKCS12 Format）] または [PEM 形式（PEM Format）] をクリックすることにより、証明書の形式を選択します。	
ステップ 8	PKCS12 ファイルをエクスポート用に暗号化するために使用する暗号化パスフレーズを入力します。	
ステップ 9	暗号化パスフレーズを確認のために再入力します。	

	コマンドまたはアクション	目的
ステップ 10	[エクスポート（Export）] をクリックして、証明書コンフィギュレーションをエクスポートします。	情報ダイアログボックスが表示され、証明書コンフィギュレーション ファイルが指定の場所に正常にエクスポートされたことが示されます。

インストールされた証明書の編集

インストールされている証明書の詳細オプションのみを変更できます。

ステップ 1 ナビゲーションメニューで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 [ASA] タブをクリックします。
ステップ 4 ASA デバイスを選択し、右側の [管理] で [トラストポイント] をクリックします。
ステップ 5 変更する証明書をクリックし、右側の [アクション] ペインで [編集] をクリックします。
ステップ 6 該当するパラメータを変更し、[保存（Save）] をクリックします。

ASA から既存証明書を削除する

証明書は 1 つずつ削除できます。証明書を削除すると、復元できなくなります。

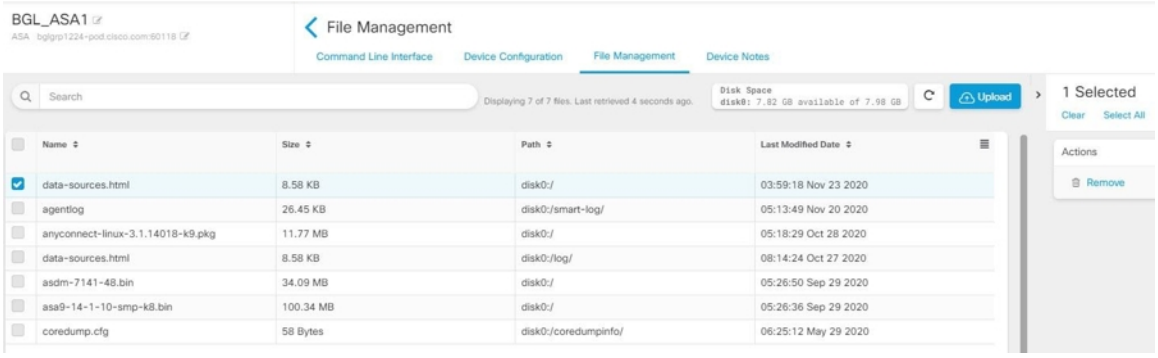
ステップ 1 ナビゲーションメニューで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 ASA デバイスを選択し、右側の [管理（Management）] で [トラストポイント（Trustpoints）] をクリックします。
ステップ 3 変更する証明書をクリックし、右側の [アクション] ペインで [削除] をクリックします。
ステップ 4 [OK] をクリックして、選択した証明書を削除します。

ASA ファイルの管理

CDO は、ASA デバイスのフラッシュ（disk0）スペースに存在するファイルの表示、アップロード、または削除などの基本的なファイル管理タスクを実行するために役立つファイル管理ツールを提供します。

（注） disk1 に存在するファイルを管理することはできません。

[ファイル管理（File Management）]画面には、デバイスのフラッシュ（disk0）に存在するすべてのファイルが一覧表示されます。ファイルのアップロードが成功したら、更新のアイコンをクリックしてファイルを表示することができます。デフォルトでは、この画面は 10 分ごとに自動的に更新されます。[ディスク容量（Disk Space）] フィールドには、disk0 ディレクトリのディスク容量が表示されます。



AnyConnect イメージは、単一または複数の ASA デバイスにアップロードできます。アップロードが成功すると、AnyConnect イメージは、選択した ASA デバイスの RA VPN 設定に関連付けられます。これにより、容易に、新しくリリースされた AnyConnect パッケージを複数の ASA デバイスに同時にアップロードできます。

フラッシュシステムへのファイルのアップロード

CDO は、リモートサーバーからの URL ベースのファイルアップロードのみをサポートしています。ファイルをアップロードするためにサポートされているプロトコルは、HTTP、HTTPS、TFTP、FTP、SMB、および SCP です。AnyConnect ソフトウェアイメージ、DAP.xml、data.xml、ホストスキャンイメージファイルなどの任意のファイルを単一または複数の ASA デバイスにアップロードできます。

（注） リモートサーバーの URL パスが無効である場合または何らかの問題が発生した問題、CDO は、選択された ASA デバイスにファイルをアップロードしません。詳細については、そのデバイスの [ワークフロー（Workflows）] に移動してください。

デバイスがハイアベイラビリティ用に設定されている場合、CDO は、まずファイルをスタンバイデバイスにアップロードし、そのアップロードが成功した後にのみ、アクティブデバイスにファイルがアップロードされます。ファイル削除プロセスでも同じ動作が適用されます。

ファイルのアップロード時にサポートされているプロトコルの構文:

プロトコル（Protocol）	構文	例
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html

プロトコル（Protocol）	構文	例
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	[illegible]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/filename]	scp://rootcisco123@10.10.166//root/events_send.py

はじめる前に

- ASA デバイスからリモートサーバーにアクセスできることを確認します。
- ファイルがすでにリモートサーバーにアップロードされていることを確認します。
- ASA デバイスからそのサーバーへのネットワークルートがあることを確認します。
- URL で FQDN が使用されている場合は、DNS が設定されていることを確認します。
- リモートサーバーの URL は、認証を求めない直接リンクである必要があります。
- リモートサーバーの IP アドレスが NAT 処理されている場合は、リモートサーバーのロケーションの NAT 処理済みパブリック IP アドレスを指定する必要があります。

（注） フェールオーバーでピアとして設定されている ASA にファイルをアップロードすると、CDO はフェールオーバーペアの他のピアの新しいファイルを確認せず、デバイスのステータスは **[未同期（Not Synced）]** に変わります。CDO が両方のデバイスのファイルを認識できるようにするには、変更を**両方**のデバイスに手動で展開する必要があります。

単一の ASA デバイスへのファイルのアップロード

単一の ASA デバイスにファイルをアップロードするには、この手順を使用します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 右側の [管理] ペインで、[ファイル管理（File Management）] をクリックします。使用可能なディスクスペースと ASA デバイスに存在するファイルが表示されます。

ステップ 5 右側の [アップロード] ボタンをクリックします。

ステップ 6 **URL リンク**で、ファイルが事前にアップロードされているサーバーのパスを指定します。[接続先パス（Destination Path）] フィールドには、**disk0** ディレクトリにアップロードされるファイルの名前が表示されます。disk0 内の特定のディレクトリにファイルをアップロードする場合は、このフィールドでその名前を指定します。たとえば、dap.xml ファイルを「DAPFiles」ディレクトリにアップロードする場合は、フィールドで「**disk0:/**DAPFiles/dap.xml」と指定します。

（注） CDO ASA CLI インターフェイスで **dir** コマンドを実行すると、disk0 フォルダに存在するディレクトリが表示されます。

ステップ 7 指定したサーバーパスが AnyConnect ファイルを指している場合、[ファイルを RA VPN 設定に関連付ける（Associate file with RA VPN Configuration）] チェックボックスがオンになります。**注**：このチェック ボックスは、正しい命名規則（「anyconnect-win-xxx.pkg」、「anyconnect-linux-xxx.pkg」、または「anyconnect-mac-xxx.pkg」形式）に従う AnyConnect ファイル名に対してのみ有効です。このチェックボックスを選択すると、アップロードが成功した後、CDO は AnyConnect ファイルを選択した ASA デバイスの RA VPN 設定に関連付けます。

ステップ 8 [アップロード（Upload）] をクリックします。CDO がファイルをデバイスにアップロードします。

ステップ 9 手順 5 で AnyConnect パッケージの RA VPN 設定との関連付けを選択した場合は、CDO から ASA に設定変更を展開します。。

次のタスク

設定の変更をデバイスに展開する必要はありません。

複数の ASA デバイスへのファイルのアップロード

複数の ASA デバイスにファイルを同時にアップロードするには、この手順を使用します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [ASA] タブをクリックし、複数の ASA デバイスを選択して一括アップロードを実行します。

ステップ 4 右側の [デバイスアクション] ペインで、[ファイルのアップロード（Upload File）] をクリックします。注：[ファイルのアップロード（Upload File）] リンクは、ASA デバイスがオンラインの場合に表示されます。

ステップ 5 [URL リンク（URL link）]で、ファイルが事前にアップロードされているサーバーのパスを指定します。[接続先パス（Destination Path）] フィールドには、**disk0** ディレクトリにアップロードされるファイルの名前が表示されます。disk0 内の特定のディレクトリにファイルをアップロードする場合は、このフィールドでその名前を指定します。たとえば、dap.xml ファイルを「DAPFiles」ディレクトリにアップロードする場合は、フィールドで「**disk0:**/DAPFiles/dap.xml」と指定します。

（注） CDO ASA CLI インターフェイスで **dir** コマンドを実行すると、disk0 フォルダに存在するディレクトリが表示されます。

ステップ 6 指定したサーバーパスが AnyConnect ファイルを指している場合、[ファイルをRA VPN設定に関連付ける（Associate file with RA VPN Configuration）] チェックボックスがオンになります。

（注） このチェック ボックスは、正しい命名規則（「anyconnect-win-xxx.pkg」、「anyconnect-linux-xxx.pkg」、または「anyconnect-mac-xxx.pkg」形式）に従う AnyConnect ファイル名に対してのみ有効です。このチェックボックスを選択すると、アップロードが成功した後、CDO は AnyConnect ファイルを選択した ASA デバイスの RA VPN 設定に関連付けます。

ステップ 7 [アップロード（Upload）] をクリックします。

ステップ 8 手順 4 で AnyConnect パッケージの RA VPN 設定との関連付けを選択した場合は、CDO から ASA に設定変更を展開します。。

次のタスク

個々のデバイスのファイルのアップロードの進行状況を表示できます。ASA デバイスを選択し、右側の [管理] ペインで [ファイル管理（File Management）] をクリックします。ファイルのアップロードが進行中の場合は、操作が完了するまで待ちます。

設定の変更をデバイスに展開する必要はありません。

ASA からのファイルの削除

RA VPN 設定に関連付けられた AnyConnect ファイルを削除することはできません。対応する RA VPN 設定から AnyConnect ファイルの関連付けを解除してから、ファイル管理ツールからファイルを削除する必要があります。

（注） フェールオーバーでピアとして設定されている ASA にファイルをアップロードすると、CDO はフェールオーバーペアの他のピアの新しいファイルを確認せず、デバイスのステータスは **[未同期（Not Synced）]** に変わります。CDO が両方のデバイスのファイルを認識できるようにするには、変更を**両方**のデバイスに手動で展開する必要があります。

remove の操作は、選択したファイルをフラッシュメモリから完全に削除します。ファイルの削除時に確認を求めるメッセージが表示されます。選択した ASA デバイスからファイルを削除するには、次の手順を使用します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 [ASA] タブをクリックして、ASA デバイスを選択します。

ステップ 4 右側の [管理] ペインで、[ファイル管理（File Management）] をクリックします。

ステップ 5 削除するファイルを選択し、右側の [アクション] で [削除] をクリックします。最大 25 個のファイルを選択できます。CDO が一部のファイルの削除に失敗した場合は、デバイスの**ワークフロー**を表示して、削除されたファイルと保持されたファイルを確認できます。

ステップ 6 AnyConnect パッケージの削除を選択した場合は、CDO から ASA に設定変更を展開します。。

ASA の高可用性を管理する

アクティブ-アクティブ フェールオーバー モードの ASA に加えられた設定変更

Cisco Defense Orchestrator（CDO）が ASA の実行構成を CDO でステージングされた構成で変更する場合、または CDO の構成を ASA に保存されている構成で変更する場合、CDO は、設定の変更部分が CDO GUI で管理可能な場合、構成ファイルの関連する行のみを変更しようとします。CDO GUI を使用して目的の構成変更を行うことができない場合、CDO は構成ファイル全体を上書きして変更を加えようとします。

2 つの例を示します。

- ネットワークオブジェクトは、CDO GUI を使用して作成または変更が可能です。CDO がその変更を ASA の設定に展開する必要がある場合、変更が発生したときに ASA の実行構成ファイルの関連する行が上書きされます。
- CDO GUI を使用して新しい ASA ユーザーを作成することはできません。ASA の ASDM または CLI を使用して新しいユーザーが ASA に追加された場合、そのアウトオブバンド変更が受け入れられ、CDO が保存されているコンフィギュレーション ファイルを更新すると、CDO は CDO にステージングされているその ASA のコンフィギュレーション ファイル全体を上書きしようとします。

ASA がアクティブ-アクティブ フェールオーバー モードで設定されている場合、これらのルールは適用されません。CDO がアクティブ-アクティブ フェールオーバー モードで設定された ASA を管理する場合、CDO は常に、すべての設定変更をそれ自体から ASA に展開したり、すべての設定変更を ASA からそれ自体に読み込むとは限りません。これに該当する 2 つの例を次に示します。

- CDO が CDO GUI でサポートしていない、CDO で行われた ASA の設定ファイルへの変更は、ASA に展開できません。また、CDO がサポートしていない設定ファイルに加えられた変更と、CDO がサポートしている設定ファイルに加えられた変更の組み合わせは、ASA に展開できません。どちらの場合も、「CDO は現時点でフェールオーバーモードのデバイスの完全な構成の置き換えをサポートしていません。[キャンセル]をクリックして、デバイスに手動で変更を適用してください。」というエラーメッセージを受け取ります。CDO インターフェイスのメッセージとともに、無効になっている [構成の置換（Replace Configuration）] ボタンが表示されます。
- アクティブ-アクティブ フェールオーバー モードで設定された ASA に加えられたアウトオブバンド変更は、CDO によって拒否されません。ASA の実行構成にアウトオブバンド変更を加えると、ASA は[デバイスとサービス]ページで「競合が検出されました（Conflict Detected）」とマークされます。競合を確認して拒否しようとすると、CDO はそのアクションをブロックします。「CDO は、このデバイスのアウトオブバンド変更の拒否をサポートしていません。このデバイスは、サポートされていないソフトウェアバージョンを実行しているか、アクティブ/アクティブ フェールオーバー ペアのメンバーです。[続行]

をクリックして、アウトオブバンド変更を受け入れてください。」というエラーメッセージを受け取ります。

⚠

注意 ASA からのアウトオブバンド変更を受け入れることにした場合、CDO でステージングされていて、まだ ASA に展開されていない設定変更はすべて上書きされ、失われます。

変更が CDO GUI でサポートされている場合、CDO は、フェールオーバーモードの ASA に加えられた設定変更をサポートします。

関連情報：

ASA での DNS の設定

次の手順を使用して、各 ASA でドメインネームサーバー（DNS）を設定します。

前提条件

- ASA はインターネットにアクセスできる必要があります。
- 開始する前に、次の情報を収集します。
  - DNS サーバーに到達できる ASA インターフェイスの名前。たとえば、inside、outside、dmz。
  - 組織で使用する DNS サーバーの IP アドレス。独自の DNS サーバーを保持していない場合は、Cisco Umbrella を使用できます。Cisco Umbrella の IP アドレスは 208.67.220.220 です。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
ステップ 3 [ASA] タブをクリックし、DNS を設定するすべての ASA を選択します。
ステップ 4 右側の操作ウィンドウで、[コマンド ライン インターフェイス] を選択します。
ステップ 5 CLI マクロのお気に入りの星をクリックします。
ステップ 6 [マクロ] パネルで [DNSの設定] マクロを選択します。
ステップ 7 [>_パラメータを表示] を選択し、パラメータ列に以下のパラメータの値を入力します。

- IF_Name：DNS サーバーに到達できる ASA インターフェイスの名前。
- IP_ADDR： 組織で使用する DNS サーバーの IP アドレス。

ステップ 8 [デバイスに送信] をクリックします。

CDO コマンド ライン インターフェイスを使用する

CDO では、コマンド ライン インターフェイス（CLI）を使用して ASA デバイスを管理できます。コマンドは、単一のデバイスに送信することも、複数のデバイスに同時に送信することも可能です。ここでは、CLI コマンドを単一の ASA デバイスに送信する方法について説明します。

関連情報：

- 詳細な ASA CLI ドキュメントについては、ASA コマンド ライン インターフェイスのドキュメント を参照してください。

コマンドの入力方法

1 つのコマンドを 1 行に入力することも、複数のコマンドを複数の行に連続して入力することも可能で、CDO は、入力されたコマンドをバッチとして順番に実行します。次の ASA の例では、3つのネットワークオブジェクトと、それらのネットワークオブジェクトを含むネットワーク オブジェクト グループを作成するコマンドのバッチを送信します。

[ASAデバイスコマンドの入力（Entering ASA device Commands）]：CDO は、グローバル コンフィギュレーション モードでコマンドの実行を開始します。

長いコマンド：非常に長いコマンドを入力すると、CDO は、コマンドを複数のコマンドに分割して、すべてのコマンドを ASA API に対して実行できるようにします。コマンドの適切な区切りを CDO が判断できない場合、コマンドのリストをどこで区切るかのヒントを求めるプロンプトが表示されます。次に例を示します。

```
Error: CDO attempted to execute a portion of this command with a length that exceeded
600 characters. You can give a hint to CDO at where a proper command separation point
is by breaking up your list of commands with an additional empty line between them.
```

このエラーメッセージを受信した場合、次の手順を実行します。

ステップ 1 CLI 履歴ペインでエラーの原因となったコマンドをクリックします。CDO は、コマンドボックスにコマンドの長いリストを入力します。

ステップ 2 関連するコマンドのグループの後に空行を挿入して、コマンドの長いリストを編集します。たとえば、上記の例のように、ネットワークオブジェクトのリストを定義し、それらをグループに追加した後に空の行を追加します。この作業を、コマンドリストのいくつかの箇所で実行することになる場合があります。

ステップ 3 [送信（Send）] をクリックします。

単一デバイスで CLI を使用する

ステップ 1 [デバイスとサービス] ページを開きます。

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 コマンド ライン インターフェイスを使用して、管理するデバイスを選択します。

ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 上部の「コマンドペイン」にコマンドを入力し、[送信（Send）] をクリックします。 コマンドに対するデバイスの応答は、「応答ペイン」の下に表示されます。

（注） 選択したデバイスが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

コマンド履歴での動作

CLI コマンドを送信すると、CDO はそのコマンドを [コマンド ライン インターフェイス（Command Line Interface）] ページの履歴ペインに記録します。履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することもできます。

ステップ 1 [デバイスとサービス] ページで、設定するデバイスを選択します。

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 [>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 履歴ペインがまだ展開されていない場合は、時計アイコン をクリックして展開します。

ステップ 6 [履歴（History）] ペインで変更または再送信するコマンドを選択します。

ステップ 7 コマンドをそのまま再利用するか、コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。CDO は、応答ペインにコマンドの結果を表示します。

（注） 次の 2 つの状況で「完了しました（Done!）」というメッセージが CDO の応答ペインに表示されます。

- コマンドがエラーなしで正常に実行された後。
- コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「完了しました（Done!）」を返します。

ASA デバイスの構成

ASA など、一部のタイプのデバイスは、構成を 1 つの構成ファイルに保存します。 これらのデバイスの場合、Cisco Defense Orchestrator でデバイス構成ファイルを表示し、デバイスに応じてさまざまな操作を実行できます。

デバイスの構成ファイルを表示する

ASA、Cisco Secure Firewall Cloud Native、SSH 管理対象デバイス、Cisco IOS を実行しているデバイスなど、構成全体を 1 つの構成ファイルに保存するデバイスの場合、CDO を使用して構成ファイルを表示できます。

（注） SSH 管理対象デバイスと Cisco IOS デバイスには読み取り専用の設定があります。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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 設定を表示するデバイスまたはモデルを選択します。

ステップ 5 右側の [管理（Management] ペインで、[設定（Configuration）] をクリックします。
完全な構成ファイルが表示されます。

関連情報：

- デバイス構成ファイルの編集

完全なデバイス設定ファイルの編集

ASA など、一部のタイプのデバイスは、設定を1つの構成ファイルに保存します。これらのデバイスの場合、CDO でデバイス構成ファイルを表示し、デバイスに応じてさまざまな操作を実行できます。

現在、CDO を使用して直接編集できるのは構成ファイルのみです。ASA

⚠

注意 この手順は、デバイスの構成ファイルのシンタックスに精通している上級ユーザーを対象としています。この手法では、Defense Orchestrator に保存されている構成ファイルのコピーに直接変更を加えます。

手順

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] 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] 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 [ASA] タブをクリックします。

ステップ 4 構成を編集するデバイスを選択します。

ステップ 5 右側の [管理] ペインで、[構成] をクリックします。

ステップ 6 [デバイスの構成] ページで、[編集] をクリックします。

ステップ 7 右側のエディタボタンをクリックして、**デフォルト**のテキストエディタ、**Vim**、または **Emacs** テキストエディタを選択します。

ステップ 8 ファイルを編集し、変更を保存します。

ステップ 9 [デバイスとサービス] ページに戻り、変更をプレビューして展開します。

ASA 構成の比較

2 つの ASA の構成を比較するには、次の手順を実行します。

ステップ 1 ナビゲーションメニューで、[デバイスとサービス（Devices & Services）] をクリックします。

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

ステップ 3 [ASA] タブをクリックします。

ステップ 4 比較するデバイスを見つけるためにデバイスリストをフィルタ処理します。

ステップ 5 2 つの ASA を選択します。それらのステータスは重要ではありません。Defense Orchestrator に保存されている ASA の構成を比較しようとしています。

ステップ 6 右側の [デバイスアクション] ペインで、[比較] をクリックします。

ステップ 7 [構成の比較（Comparing Configurations）] ダイアログで、[次へ] および [前へ（Previous）] をクリックして、構成ファイル内の青色で強調表示されている相違点をスキップします。

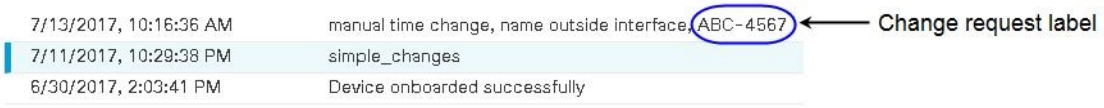
ASA 設定の復元

この手順では、Cisco Defense Orchestrator（CDO）を使用して ASA に行った設定変更を復元する方法について説明します。これは、予期しない結果や望ましくない結果をもたらした設定変更を削除する便利な方法です。

設定を復元する前に

設定を復元する前に、次の注意事項を確認してください。

- CDO は、復元することを選択した設定を、ASA に展開されている最後に認識された設定と比較します。ステージングされているが ASA のメモリに展開されていない設定とは比較しません。ASA に展開されていない変更がある場合に、以前の設定を復元すると、展開されていない変更は、復元プロセスによって上書きされて失われます。
- 過去の設定を復元すると、それまでに展開されたすべての設定変更が上書きされます。たとえば、以下のリストにある 2017 年 7 月 11 日の設定を復元すると、2017 年 7 月 13 日に行われた設定変更が上書きされます。



- 設定変更に最初に適用した変更リクエストラベルは、[設定の復元（Restore Configuration）] リストに表示されます。
- ASA は [同期（Synced）] または [非同期] の状態になっている可能性があるため、過去の設定を復元する前に、設定の競合を解決する必要があります。

設定の復元方法

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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 [ASA] タブをクリックします。

ステップ 4 設定を復元する ASA を選択します。

ステップ 5 右側のペインで **[設定（Configuration）]** > **[設定の復元（Restore Configuration）]** を選択します。

ステップ 6 [設定の復元（Restore Configuration）] ペインで、復元する設定を選択します。たとえば、上の図では、2017 年 7 月 11 日の設定が選択され、強調表示されています。

ステップ 7 「CDO によって検証された最新の実行設定」と「*<date>* から選択された設定」を比較して、[<date> から選択された設定（Selected Configuration from *<date>*）] ウィンドウに表示されている設定を復元することを確認します。

ステップ 8 [復元（Restore）] をクリックします。これにより、CDO の設定がステージングされます。[デバイスとサービス] ページに、デバイスの設定ステータスが [非同期] と表示されます。

ステップ 9 右側のペインで [変更の展開 ...（Deploy Changes...）] をクリックして変更を展開し、ASA を同期させます。

トラブルシューティング

保持したかったのに失ってしまった変更を回復するには、どうすればよいですか。

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] 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] 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 [ASA] タブをクリックします。

ステップ 4 必要なデバイスを選択します。

ステップ 5 右側のペインで [変更ログ] をクリックします。

ステップ 6 変更ログで変更を確認します。それらの記録から、失われた構成を再構築できる可能性があります。

CLI を使用した ASA の設定

CDO で提供される CLI インターフェイスで CLI コマンドを実行して、ASA デバイスを設定できます。このインターフェイスを使用するには、[デバイスとサービス] メニューでデバイスを選択し、[コマンド ライン インターフェイス（Command Line Interface）] をクリックします。詳細については、「CDO コマンド ライン インターフェイスの使用」を参照してください。

新しいロギングサーバーの追加

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。

詳細については、実行している ASA バージョンの『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』に含まれる「Logging」の章にある「Monitoring」セクションを参照してください。

DNS サーバーの設定

DNS サーバーを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセスルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するように、DNS サーバーを設定する必要があります。

詳細については、実行している ASA バージョンの『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』に含まれる「Basic Settings」の章の「Configure the DNS Server」セクションを参照してください。

静的ルートとデフォルトルートの追加

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティックルーティングとダイナミックルーティングのどちらかを使用して、ホストまたはネットワークへのルートを定義する必要があります。

詳細については、『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』の「Static and Default Routes」の章を参照してください。

インターフェイスの設定

CLI コマンドを使用して、管理インターフェイスとデータインターフェイスを設定できます。詳細については、『CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide』の「Basic Interface Configuration」の章を参照してください。

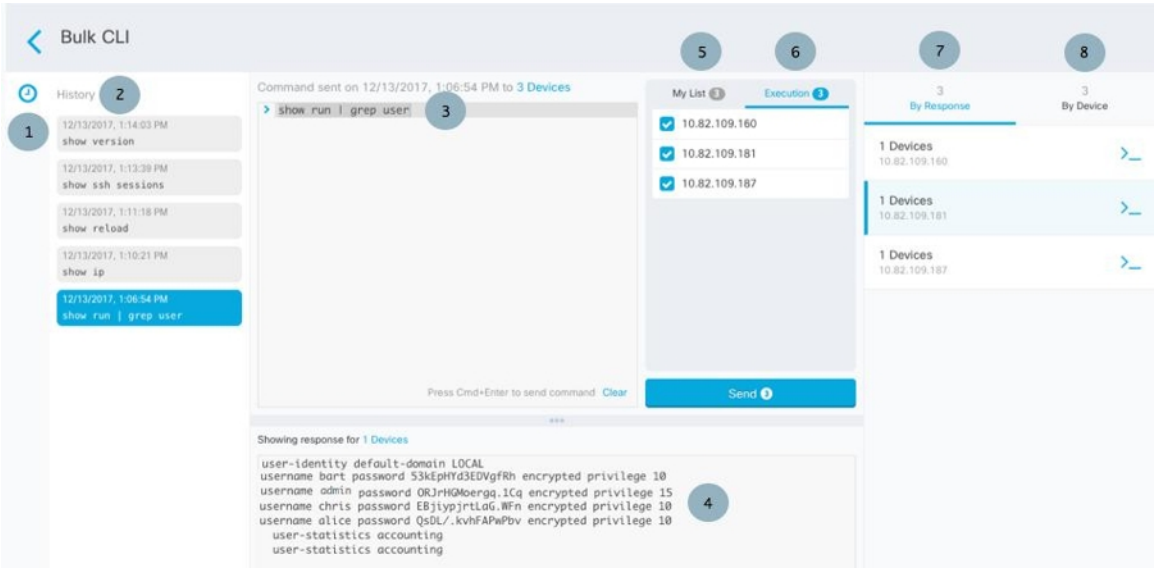
一括コマンド ライン インターフェイス

CDO では、コマンド ライン インターフェイス（CLI）を使用して ASA デバイスを管理できます。コマンドは、単一のデバイスに送信することも、同じ種類の複数のデバイスに同時に送信することも可能です。この項目では、CLI コマンドを複数のデバイスに一度に送信する方法について説明します。

関連情報：

- 詳細な ASA CLI のドキュメントについては、ASA コマンド ライン インターフェイスのドキュメントを参照してくださ
- Cisco IOS CLI のドキュメントについては、お使いの IOS バージョンの「Networking Software（IOS & NX-OS）」を参照してください。https://www.cisco.com/c/en/us/support/ios-nx-os-software/index.html

一括 CLI インターフェイス



（注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。

- コマンドがエラーなしで正常に実行された後。
- コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「**完了しました（Done!）**」を返します。

ケース	説明
1	コマンド履歴ペインを展開したり折りたたんだりするには、時計アイコンをクリックします。
2	コマンド履歴。コマンドを送信すると、CDO はこの履歴ペインにコマンドを記録するので、コマンドをもう一度選択し、再度実行できます。
3	コマンドペイン。このペインのプロンプトにコマンドを入力します。

ケース	説明
4	応答ペイン。CDO は、コマンドに対するデバイスの応答と CDO メッセージを表示します。複数のデバイスの応答が同じだった場合、応答ペインに「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。 （注） 次の 2 つの状況で「**完了しました（Done!）**」というメッセージが CDO に表示されます。 • コマンドがエラーなしで正常に実行された後。 • コマンドの返すべき結果が何もなかった場合。たとえば、特定の設定エントリを検索する正規表現を含む show コマンドを発行したとします。この正規表現の条件に合致する設定エントリがなかった場合、CDO は「**完了しました（Done!）**」を返します。
5	[マイリスト] タブには、[インベントリ] テーブルから選択したデバイスが表示されます。このタブで、コマンドを送信するデバイスを含めたり除外したりすることができます。
[6]	上の図で強調表示されている [実行（Execution）] タブには、履歴ペインで選択されているコマンドの対象デバイスが表示されます。この例では、履歴ペインで show run | grep user コマンドが選択され、[実行（Execution）] タブに、10.82.109.160、10.82.109.181、および 10.82.10.9.187 に送信されたことが表示されます。
7	[応答別（By Response）] タブをクリックすると、コマンドによって生成された応答のリストが表示されます。同一の応答は 1 行にグループ化されます。[応答別] タブで行を選択すると、CDO はそのコマンドへの応答を応答ペインに表示します。
8	[デバイス別（By Device）] タブをクリックすると、各デバイスからの個別の応答が表示されます。リスト内のいずれかのデバイスをクリックすると、特定のデバイスからのコマンドへの応答を表示できます。

コマンドの一括送信

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックして、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 CLI を使用して管理するデバイスを特定して、それらを選択します。

ステップ 5 詳細ペインで、>_ [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 6 コマンドペインにコマンドを入力して、[送信（Send）] をクリックします。コマンド出力が応答ペインに表示されます。コマンドは変更ログに記録され、CDO はコマンドを [一括CLI（Bulk CLI）] ウィンドウの [履歴（History）] ペインに記録します。

（注） 選択したデバイスが到達可能で同期されていることを確認してください。ASA デバイスが同期されていない場合、そのデバイスで使用可能なコマンドは、`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy` だけです。

一括コマンド履歴での動作

一括 CLI コマンドを送信すると、CDO はそのコマンドを一括 CLI ページの履歴ペインに記録します。履歴ペインに保存されたコマンドは、再実行することも、コマンドをテンプレートとして使用することもできます。履歴ペインのコマンドは、それらが実行された元のデバイスに関連付けられています。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックして、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、設定するデバイスを選択します。

ステップ 4 [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 5 [履歴（History）] ペインで変更または再送信するコマンドを選択します。選択したコマンドは特定のデバイスに関連付けられており、最初のステップで選択したものとは限らないことに注意してください。

ステップ 6 [マイリスト] タブを見て、送信しようとしているコマンドが対象のデバイスに送信されることを確認します。

ステップ 7 コマンドペインでコマンドを編集し、[送信（Send）] をクリックします。CDO は、応答ペインにコマンドの結果を表示します。

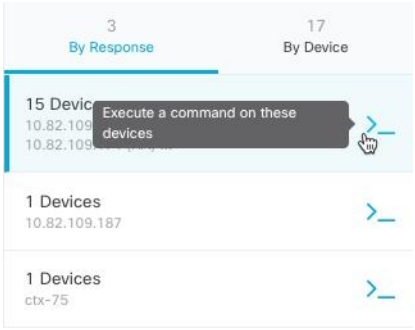
（注） 選択したデバイスのいずれかが同期されていない場合、次のコマンドのみが許可されます：`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`write`、`copy`

一括コマンドフィルタでの動作

一括 CLI コマンドを実行後、[応答別（By Response）] フィルタと [デバイス別（By Device）] フィルタを使用して、デバイスの設定を続行できます。

応答別フィルタ

一括コマンドの実行後、CDO は [応答別（By Response）] タブに、コマンドを送信したデバイスから返された応答のリストを入力します。同じ応答のデバイスは1行にまとめられます。[応答別（By Response）] タブの行をクリックすると、応答ペインにデバイスからの応答が表示されます。応答ペインに複数のデバイスの応答が表示される場合、「Xデバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが



CDO に表示されます。

コマンド応答に関連付けられたデバイスのリストにコマンドを送信するには、次の手順に従います。

ステップ 1 [応答別（By Response）] タブの行にあるコマンドシンボルをクリックします。

ステップ 2 コマンドペインでコマンドを確認し、[送信（Send）] をクリックしてコマンドを再送信するか、[クリア] をクリックしてコマンドペインをクリアし、新しいコマンドを入力してデバイスに送信してから、[送信（Send）] をクリックします。

ステップ 3 コマンドから受け取った応答を確認します。

ステップ 4 選択したデバイスの実行コンフィギュレーション ファイルに変更が反映されていることが確実な場合は、コマンドペインに「deploy memory」と入力し、[送信（Send）] をクリックします。この操作により、実行構成がスタートアップ コンフィギュレーションに保存されます。

デバイス別フィルタ

一括コマンドの実行後、CDO は [実行（Execution）] タブと [デバイス別（By Device）] タブに、コマンドを送信したデバイスのリストを入力します。[デバイス別（By Device）] タブの行をクリックすると、各デバイスの応答が表示されます。

同じデバイスリストでコマンドを実行するには、次の手順に従います。

ステップ 1 [デバイス別（By Device）] タブをクリックします。

ステップ 2 [>_これらのデバイスでコマンドを実行（>_Execute a command on these devices）] をクリックします。

ステップ 3 [クリア] をクリックしてコマンドペインをクリアし、新しいコマンドを入力します。

ステップ 4 [マイリスト] ペインで、リスト内の個々のデバイスを選択または選択解除して、コマンドを送信するデバイスのリストを指定します。

ステップ 5 [送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。応答ペインに複数のデバイスの応答が表示される場合、「X デバイスの応答を表示しています（Showing Responses for X devices）」というメッセージが表示されます。[Xデバイス（X Devices）] をクリックすると、コマンドに対して同じ応答を返したすべてのデバイスが CDO に表示されます。

ステップ 6 選択したデバイスの実行構成ファイルに変更が反映されていることが確実な場合は、コマンドペインに「deploy memory」と入力し、[送信（Send）] をクリックします。

ASA一括 CLI の使用例

次の例は、ASA デバイスに対して CDO の一括 CLI 機能を使用するときに発生する可能性のあるワークフローです。

ASA の実行構成ですべてのユーザーを表示し、いずれかのユーザーを削除する

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックしてデバイスを見つけます。

ステップ 3 [ASA] タブをクリックします。

ステップ 4 ユーザーを削除するデバイスのデバイスリストを検索およびフィルタ処理し、デバイスを選択します。

（注） 選択したデバイスが同期されていることを確認してください。デバイスが同期されていない場合、次のコマンドのみが許可されます。`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、`dir`、`copy`、および `write`。

ステップ 5 詳細ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。CDO は、[マイリスト] ペインで選択したデバイスを一覧表示します。少数のデバイスにコマンドを送信する場合は、そのリストにあるデバイスのチェックを外します。

ステップ 6 コマンドペインで、`show run | grep user` と入力し、[送信（Send）] をクリックします。文字列 user を含む実行構成ファイルのすべての行が、応答ペインに表示されます。[実行（Execution）] タブが開き、コマンドが実行されたデバイスが表示されます。

ステップ 7 [応答別（By Response）] タブをクリックし、応答を確認して、削除するユーザーが含まれているデバイスを確認します。

ステップ 8 [マイリスト] タブをクリックし、ユーザーを削除するデバイスのリストを選択します。

ステップ 9 コマンドペインで、user コマンドの no 形式を入力して user2 を削除し、[送信（Send）] をクリックします。この例では、user2 を削除します。

```
no user user2 password reallyhardpassword privilege 10
```

ステップ 10 ユーザー名の検索に使用した、`show run | grep user` コマンドのインスタンスの履歴パネルを確認します。このコマンドを選択し、[実行（Execution）] リストでデバイスのリストを確認して、[送信（Send）] を選択します。指定したデバイスからユーザー名が削除されたことがわかります。

ステップ 11 実行構成から正しいユーザーを削除し、実行構成に残っているユーザーが正しいことを確認したら、次の手順を実行します。

1. 履歴ペインから `no user user2 password reallyhardpassword privilege 10` コマンドを選択します。
2. [デバイス別（By Device）] タブをクリックし、[これらのデバイスでコマンドを実行（Execute a command on these devices）] をクリックします。
3. コマンドペインで、[クリア] をクリックしてコマンドペインをクリアします。
4. `deploy memory` コマンドを入力し、[送信（Send）] をクリックします。

選択した ASA 上のすべての SNMP 設定を見つける

この手順で、ASA の実行構成にあるすべての SNMP 構成エントリを表示できます。

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックしてデバイスを見つけます。

ステップ 3 [ASA] タブをクリックします。

ステップ 4 実行構成の SNMP 構成を分析するデバイスをフィルタ処理して検索し、それらを**選択**します。

（注） 選択したデバイスが同期されていることを確認してください。デバイスが同期されていない場合、次のコマンドのみが許可されます。`show`、`ping`、`traceroute`、`vpn-sessiondb`、`changeto`、および `dir`。

ステップ 5 詳細ペインで、[コマンド ライン インターフェイス] をクリックします。選択したデバイスは [マイリスト] ペインに表示されます。少数のデバイスにコマンドを送信する場合は、そのリストにあるデバイスのチェックを外します。

ステップ 6 コマンドペインで、`show run | grep snmp` と入力し、[送信] をクリックします。文字列 snmp を含む実行構成ファイルのすべての行が、応答ペインに表示されます。[実行] タブが開き、コマンドが実行されたデバイスが表示されます。

ステップ 7 応答ペインでコマンド出力を確認します。

デバイスの管理用 CLI マクロ

CLI マクロは、すぐに使用できる完全な形式の CLI コマンド、または実行前に変更できる CLI コマンドのテンプレートです。すべてのマクロは、1 つ以上の ASA デバイスで同時に実行できます。

テンプレートに似た CLI マクロを使用して、複数のデバイスで同じコマンドを同時に実行します。CLI マクロは、デバイスの設定と管理の一貫性を促進します。完全な形式の CLI マクロを

使用して、デバイスに関する情報を取得します。ASA デバイスですぐに使用できるさまざまな CLI マクロがあります。

頻繁に実行するタスクを監視するための CLI マクロを作成できます。詳細については、「CLI マクロの作成」を参照してください。

CLI マクロは、システム定義またはユーザー定義です。システム定義マクロは CDO によって提供され、編集も削除もできません。ユーザー定義マクロはユーザーが作成し、編集または削除できます。

（注） デバイスが CDO に導入準備された後にのみ、デバイスのマクロを作成できます。

例として ASA を使用すると、いずれかの ASA で特定のユーザーを検索する場合は、次のコマンドを実行できます。

```
show running-config | grep username
```

このコマンドを実行すると、検索しているユーザーのユーザー名が username に置き換わります。このコマンドからマクロを作成するには、同じコマンドを使用して、username を中括弧で囲みます。

```
> show running-config | grep {{username}}
```

パラメータには任意の名前を付けることができ、そのパラメータ名で同じマクロを作成することもできます。

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

パラメータ名は説明的な名前にでき、英数字と下線を使用する必要があります。この場合、コマンドシンタックスは次のようになります。

```
show running-config | grep
```

コマンドの一部として、コマンドの送信先のデバイスに適した CLI シンタックスを使用する必要があります。

新規コマンドからの CLI マクロの作成

ステップ 1 CLI マクロを作成する前に CDO のコマンド ライン インターフェイスでコマンドをテストして、コマンドの構文が正しく、信頼できる結果が返されることを確認します

（注）
- 詳細な ASA CLI ドキュメントについては、ASA コマンドライン インターフェイスのドキュメント を参照してください。

ステップ 2 ナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 3 [デバイス] タブをクリックしてデバイスを見つけます。

ステップ 4 適切なデバイスタイプのタブをクリックし、オンラインで同期されているデバイスを選択します。

ステップ 5 [>_コマンド ライン インターフェイス] をクリックします。

ステップ 6 CLI マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。

ステップ 7 プラスボタン をクリックします。

ステップ 8 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 9 [コマンド] フィールドに完全なコマンドを入力します。

ステップ 10 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 11 [作成（Create）]をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、『デバイスでの CLI マクロの実行』を参照してください。

CLI 履歴または既存の CLI マクロからの CLI マクロの作成

この手順では、すでに実行したコマンド、別のユーザー定義マクロ、またはシステム定義マクロからユーザー定義マクロを作成します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

（注） CLI 履歴からユーザー定義マクロを作成する場合は、コマンドを実行したデバイスを選択します。CLI マクロは、同じアカウントのデバイス間で共有されますが、CLI 履歴は共有されません。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、オンラインかつ同期されているデバイスを選択します。

ステップ 4 [>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

ステップ 5 CLI マクロを作成するコマンドを見つけて選択します。次のいずれかの方法を使用してください。

- クロック をクリックして、そのデバイスで実行したコマンドを表示します。マクロに変換するコマンドを選択すると、コマンドペインにそのコマンドが表示されます。
- CLI マクロのお気に入りのスター をクリックして、すでに存在するマクロを確認します。変更するユーザー定義またはシステム定義の CLI マクロを選択します。コマンドがコマンドペインに表示されます。

ステップ 6 コマンドがコマンドペインに表示された状態で、CLI マクロの金色の星 をクリックします。このコマンドが、新しい CLI マクロの基礎になります。

ステップ 7 マクロに一意の名前を指定します。必要に応じて、CLI マクロの説明とメモを入力します。

ステップ 8 [コマンド] フィールドのコマンドを確認し、必要な変更を加えます。

ステップ 9 コマンドの実行時に変更したいコマンドの部分を、中括弧で囲まれたパラメータ名に置き換えます。

ステップ 10 [作成（Create）]をクリックします。作成したマクロは、最初に指定したデバイスだけでなく、そのタイプのすべてのデバイスで使用できます。

コマンドを実行するには、CLI マクロの実行を参照してください。

CLI マクロの実行

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブをクリックし、1 つ以上のデバイスを選択します。

ステップ 4 [>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

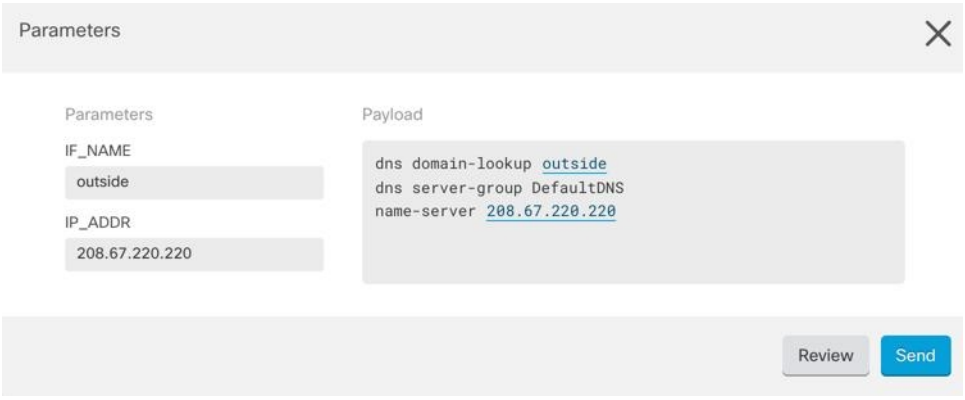
ステップ 5 コマンドパネルで、スター をクリックします。

ステップ 6 コマンドパネルから CLI マクロを選択します。

ステップ 7 次のいずれかの方法でマクロを実行します。

- 定義するパラメータがマクロに含まれていない場合は、[送信（Send）] をクリックします。コマンドへの応答が応答ペインに表示されます。これで完了です。
- マクロにパラメータが含まれている場合（下の Configure DNS マクロなど）、[>_ パラメータの表示（>_ View Parameters）] をクリックします。

ステップ 8 [パラメータ（Parameters）] ペインで、パラメータの値を [パラメータ（Parameters）] の各フィールドに入力します。



ステップ 9 [送信（Send）] をクリックします。CDO が正常にコマンドを送信し、デバイスの構成を更新すると、「Done!」というメッセージが表示されます。

- ASA の場合は、実行構成が更新されます。

ステップ 10 コマンドを送信した後で、「一部のコマンドが実行構成に変更を加えた可能性があります」というメッセージが 2 つのリンクとともに表示されることがあります。

- [ディスクへの書き込み（Write to Disk）] をクリックすると、このコマンドによって加えられた変更と、実行構成のその他の変更がデバイスのスタートアップ構成に保存されます。
- [取り消す（Dismiss）] をクリックすると、メッセージが取り消されます。

CLI マクロの編集

ユーザー定義の CLI マクロは編集できますが、システム定義のマクロは編集できません。CLI マクロを編集すると、すべての ASA デバイスでマクロが変更されます。マクロは特定のデバイス固有のものではありません。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
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 デバイスを選択します。
ステップ 5 [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。
ステップ 6 編集するユーザー定義マクロを選択します。
ステップ 7 マクロラベルの編集アイコンをクリックします。
ステップ 8 [マクロの編集（Edit Macro）] ダイアログボックスで CLI マクロを編集します。
ステップ 9 [**保存（Save）**] をクリックします。

CLI マクロの実行方法については、「CLI マクロの実行」を参照してください。

CLI マクロの削除

ユーザー定義の CLI マクロは削除できますが、システム定義のマクロは削除できません。CLI マクロを削除すると、すべてのデバイスでマクロが削除されます。マクロは特定のデバイス固有のものではありません。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
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 デバイスを選択します。

ステップ 5 [コマンドラインインターフェイス（Command Line Interface）] をクリックします。
ステップ 6 削除するユーザー定義 CLI マクロを選択します。
ステップ 7 CLI マクロラベルのゴミ箱アイコン をクリックします。
ステップ 8 CLI マクロを削除することを確認します。

ASA コマンド ライン インターフェイスのドキュメント

CDO は、ASA コマンドラインインターフェイスをすべてサポートしています。ユーザーが単一のデバイスおよび複数のデバイスに同時にコマンドを送信できるように、CDO ではターミナル型のインターフェイスを提供しています。ASA コマンドラインインターフェイスのドキュメントは豊富です。CDO ドキュメントでその一部を再作成するのではなく、Cisco.com の ASA CLI ドキュメントへのポインタを次に示します。

ASA CLI コンフィギュレーション ガイド

ASA バージョン 9.1 以降、ASA CLI コンフィギュレーション ガイドは 3 部に分かれています。

- CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）
- CLI ブック 2: Cisco ASA シリーズ ファイアウォール CLI コンフィグレーションガイド
- 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

[サポート（Support）] > [製品カテゴリ（Products by Category）] > [セキュリティ（Security）] >[ファイアウォール（Firewalls）] > [ASA 5500] > [コンフィギュレーション（Configure）] > [コンフィギュレーションガイド（Configuration Guides）] に移動すると、Cisco.com の ASA CLI コンフィギュレーション ガイドにアクセスできます。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

いくつかの特定の ASA CLI コンフィギュレーション ガイドのセクション

show コマンドと more コマンドの出力のフィルタリングCLI ブック 1：『Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）』の「show コマンドと more コマンドの出力のフィルタリング」では、正規表現を使用した show コマンド出力のフィルタ処理について学習できます。

ASA コマンドリファレンス

ASA コマンド リファレンス ガイドは、すべての ASA コマンドとそのオプションがアルファベット順でリストになっています。ASA コマンドリファレンスはバージョン固有ではありません。次の 4 部が公開されています。

- Cisco ASA シリーズ コマンド リファレンス、A ～ H コマンド
- Cisco ASA シリーズ コマンド リファレンス、I ～ R コマンド
- Cisco ASA シリーズ コマンド リファレンス、S コマンド

- Cisco ASA シリーズ コマンド リファレンス、T ～ Z コマンドおよび ASASM 用 IOS コマンド

[サポート（Support）] > [製品カテゴリ（Products by Category）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [ASA 5500] > [リファレンスガイド（Reference Guides）] > [コマンドリファレンス（Command References）] に移動すると、Cisco.com の ASA コマンドリファレンスガイドにアクセスできます。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html#anchor325

CLI コマンドの結果のエクスポート

スタンドアロンデバイスまたは複数のデバイスに発行されたCLIコマンドの結果をコンマ区切り値（.csv）ファイルにエクスポートして、必要に応じて情報をフィルタリングおよび並べ替えることができます。単一のデバイスまたは多数のデバイスのCLI結果を一度にエクスポートできます。エクスポートされた情報には、次のものが含まれます。

- Device
- 日付（Date）
- User
- コマンド
- 出力

CLI コマンドの結果のエクスポート

コマンドウィンドウで実行したコマンドの結果を .csv ファイルにエクスポートできます。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション] ペインで、>_ [コマンド ライン インターフェイス（Command Line Interface）] をクリックします。

ステップ 6 [コマンドラインインターフェイス（Command Line Interface）] ペインでコマンドを入力し、[送信（Send）] をクリックしてデバイスに送ります。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI マクロの結果のエクスポート

コマンドウィンドウで実行されたマクロの結果をエクスポートできます。次の手順で、1 つまたは複数のデバイスで実行された CLI マクロの結果を .csv ファイルにエクスポートします。

ステップ 1 [デバイスとサービス] ページを開きます。

ステップ 2 [デバイス] タブをクリックします。

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。

ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信（Send）] をクリックします。

ステップ 8 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

CLI コマンド履歴のエクスポート

次の手順を使用して、1 つまたは複数のデバイスの CLI 履歴を .csv ファイルにエクスポートします。

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 1 つまたは複数のデバイスを選択してハイライトします。

ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 履歴ペインがまだ展開されていない場合は、[時計（Clock）] アイコン をクリックして展開します。

ステップ 7 入力されたコマンドのウィンドウの右側で、エクスポートアイコン をクリックします。

ステップ 8 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。.csv ファイル上のコマンド出力を読み取る場合、すべてのセルを展開して、コマンドのすべての結果を表示します。

関連情報：

- CDO コマンド ライン インターフェイスを使用する

- CLI マクロの作成
- CLI マクロの削除
- CLI マクロの編集
- CLI マクロの実行
- ASA 一括 CLI の使用例
- ASA コマンド ライン インターフェイスのドキュメント
- 一括コマンド ライン インターフェイス

CLI マクロのリストをエクスポートする

コマンドウィンドウで実行されたマクロのみをエクスポートできます。次の手順で、1 つまたは複数のデバイスの CLI マクロを .csv ファイルにエクスポートします。

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
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 1 つまたは複数のデバイスを選択してハイライトします。
ステップ 5 デバイスの [デバイスアクション] ペインで、[>_コマンド ライン インターフェイス] をクリックします。
ステップ 6 CLI ウィンドウの左側のペインで、CLI マクロのお気に入りを示す星を選択します。
ステップ 7 エクスポートするマクロコマンドをクリックします。適切なパラメータを入力し、[送信] をクリックします。
ステップ 8 入力されたコマンドのウィンドウの右側でエクスポートアイコン をクリックします。
ステップ 9 .csv ファイルにわかりやすい名前を付け、ファイルをローカルファイルシステムに保存します。

変更の読み取り、破棄、チェック、および展開

デバイスを管理するために、CDO は、デバイスの設定のコピーを独自のデータベースに保存する必要があります。CDO が管理対象デバイスから設定を「読み取る」とき、CDO はデバイス設定のコピーを作成し、それを保存します。CDO が最初にデバイスの設定のコピーを読み取って保存するのは、デバイスが導入準備されたときです。以下の選択肢のように、さまざまな目的に応じて設定を読み取ります。

- [変更の破棄（Discard Changes）] は、デバイスの設定ステータスが「未同期」の場合に使用できます。未同期の状態では、デバイスの設定に対する変更が CDO で保留中になっています。このオプションを使用すると、保留中のすべての変更を取り消すことができま

す。保留中の変更は削除され、CDO は設定のコピーをデバイスに保存されている設定のコピーで上書きします。

- [変更の確認（Check for Changes）]。このアクションは、デバイスの設定ステータスが同期済みの場合に使用できます。[変更の確認（Checking for Changes）] をクリックすると、CDO は、デバイスの設定のコピーを、デバイスに保存されている設定のコピーと比較するように指示します。違いがある場合、CDO はデバイスに保存されているコピーでそのデバイスの設定のコピーをすぐに上書きします。
- [競合の確認（Review Conflict）] と [レビューなしで承認（Accept Without Review）]。 . デバイスで [競合検出] を有効にすると、CDO はデバイスに加えられた設定の変更を 10 分ごとにチェックします。https://docs.defenseorchestrator.com/Welcome_to_Cisco_Defense_Orchestrator/Basics_of_Cisco_Defense_Orchestrator/Synchronizing_Configurations_Between_Defense_Orchestrator_and_Device/0010_Conflict_Detectionデバイスに保存されている設定のコピーが変更された場合、CDO は「競合が検出されました」という設定ステータスを表示して通知します。
  - [競合の確認（Review Conflict）]。[競合の確認（Review Conflict）] をクリックすると、デバイスで直接行われた変更を確認し、それらを受け入れるか拒否するかを選択できます。
  - [レビューなしで承認（Accept Without Review）]。このアクションは、デバイスの設定の CDO のコピーを、デバイスに保存されている設定のコピーで上書きします。CDO は、上書きアクションを実行する前に、設定の 2 つのコピーの違いを確認するように求めません。

[すべて読み取り（Read All）] は一括操作です。任意の状態の複数のデバイスを選択し、[すべて読み取り（Read All）] をクリックして、CDO に保存されているすべてのデバイスの設定を、デバイスに保存されている設定で上書きすることができます。

変更の配置

デバイスの設定に変更を加えると、CDO では、加えた変更が独自のコピーに保存されます。これらの変更は、デバイスに展開されるまで CDO で「保留」されています。デバイスの設定に変更があり、それがデバイスに展開されていない場合、デバイスは未同期構成状態になります。

保留中の設定変更は、デバイスを通過するネットワークトラフィックには影響しません。変更は、CDO がデバイスに展開した後にのみ影響を及ぼします。CDO がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体を上書きすることはありません。展開は、1 つのデバイスに対して開始することも、複数のデバイスに対して同時に開始することもできます。

（注） 展開や繰り返しの展開をスケジュールできます。詳細については、自動展開のスケジュール（185 ページ）を参照してください。

[すべて破棄] は、[プレビューして展開...（Preview and Deploy..）] をクリックした後にのみ使用できるオプションです。 . [プレビューして展開（Preview and Deploy）] をクリックすると、CDO で保留中の変更のプレビューが CDO に表示されます。[すべて破棄] をクリックすると、保留中のすべての変更が CDO から削除され、選択したデバイスには何も展開されません。上述の [変更の破棄（Discard Changes）] とは異なり、保留中の変更を削除すると操作が終了します。

すべてのデバイス設定の読み取り

Cisco Defense Orchestrator（CDO）の外部にあるデバイスの設定が変更された場合、CDO に保存されているデバイスの設定と、当該デバイスの設定のローカルコピーは同じではなくなります。多くの場合、CDO にあるデバイスの設定のコピーをデバイスに保存されている設定で上書きして、設定を再び同じにしたいと考えます。[すべて読み取り（Read All）] リンクを使用して、多くのデバイスでこのタスクを同時に実行できます。

CDO によるデバイス設定の 2 つのコピーの管理方法の詳細については、「変更の読み取り、破棄、チェック、および展開」を参照してください。

[すべて読み取り（Read All）] をクリックした場合に、CDO にあるデバイスの設定のコピーがデバイスの設定のコピーで上書きされる 3 つの設定ステータスを次に示します。

- [競合検出（Conflict Detected）]：競合検出が有効になっている場合、CDO は、設定に加えられた変更について、管理するデバイスを 10 分ごとにポーリングします。CDO は、デバイスの設定が変更されたことを検出した場合、デバイスの [競合検出（Conflict Detected）] 設定ステータスを表示します。
- [同期（Synced）]：デバイスが [同期（Synced）] 状態の場合に、[すべて読み取り（Read All）] をクリックしすると、CDO はすぐにデバイスをチェックして、設定に直接変更が加えられているかどうかを判断します。[すべて読み取り（Read All）] をクリックすると、CDO はデバイスの設定のコピーを上書きすることを確認し、上書きを実行します。
- [非同期]：デバイスが [非同期] 状態の場合に、[すべて読み取り（Read All）] をクリックすると、CDO を使用したデバイスの設定に対する保留中の変更があること、および [すべて読み取り（Read All）] 操作を続行すると保留中の変更が削除されてから、CDO にある設定のコピーがデバイス上の設定で上書きされることが警告されます。この [すべて読み取り（Read All）] は、[変更の破棄（Discard Changes）] と同様に機能します。変更の破棄（188 ページ）

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 （任意）変更ログでこの一括アクションの結果を簡単に識別できるように、変更リクエストラベルを作成します。

ステップ 5 CDO を保存する設定のデバイスを選択します。CDO では、選択したすべてのデバイスに適用できるアクションのコマンドボタンのみ提供されることに注意してください。

ステップ 6 [すべて読み取り（Read All）] をクリックします。

ステップ 7 選択したデバイスのいずれかについて、CDO で設定変更がステージングされている場合、CDO は警告を表示し、設定の一括読み取りアクションを続行するかどうかを尋ねられます。[すべて読み取り（Read All）] をクリックして続行します。

ステップ 8 設定の [すべて読み取り（Read All）] 操作の進行状況については、[通知（notifications）] タブで確認します。一括操作の個々のアクションの成功または失敗に関する詳細を確認する場合は、青色の [レビュー（Review）] リンクをクリックすると、[ジョブ] ページに移動します。 [ジョブ（Jobs）] ページ

ステップ 9 変更リクエストラベルを作成してアクティブ化した場合は、他の設定変更を誤ってこのイベントに関連付けないように、忘れずにラベルをクリアしてください。

関連情報

- 変更の読み取り、破棄、チェック、および展開
- 変更の破棄
- 設定変更の確認

ASA から CDO への設定変更の読み取り

Cisco Defense Orchestrator が ASA の設定を「読み取る」理由

ASA を管理するために、CDO には、ASA の実行構成ファイルの独自のコピーが保存されている必要があります。CDO が最初にデバイスの構成ファイルのコピーを読み取って保存するのは、デバイスが導入準備されたときです。その後、CDO が ASA から設定を読み取るときに、[変更の確認（Check for Changes）]、[レビューなしで承認（Accept Without Review）]、または [設定の読み取り（Read Configuration）] のいずれかを選択します。詳細については、「変更の読み取り、破棄、チェック、および展開」を参照してください。

CDO は、次の状況でも ASA の設定を読み取る必要があります。

- ASA への設定変更の展開に失敗し、デバイスの状態がリストにないか、[非同期] になっている場合。
- デバイスの導入準備が失敗し、デバイスの状態が [設定なし（No Config）] になっている場合。
- CDO の外部でデバイス設定を変更したが、その変更はポーリングまたは検出されていないため、デバイスの状態が [同期（Synced）] または [競合検出（Conflict Detected）] になっている場合。

このような場合、CDO は、デバイスに保存されている最後に認識された設定のコピーを必要とします。

ASA での構成変更の読み取り

ASA での構成変更の読み取りが求められたら、次の手順を実行します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
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 CDO が最近導入準備に失敗したデバイス、または CDO が変更の展開に失敗したデバイスを選択します。
ステップ 5 右側の [同期済み] ペインで [構成の読み取り（Read Configuration）] をクリックします。このオプションを実行すると、現在 CDO に保存されている構成が上書きされます。

すべてのデバイスの構成変更のプレビューと展開

テナント上のデバイスに構成変更を加えたものの、その変更をまだ展開していない場合に、CDO は展開アイコンにオレンジ色のドットを表示して通知します。

.これらの変更の影響を受けるデバイスには、[デバイスとサービス]ページに[非同期]のステータスが表示されます。[展開]をクリックすると、保留中の変更があるデバイスを確認し、それらのデバイスに変更を展開できます。

この展開方法は、サポートされているすべてのデバイスで使用できます。

この展開方法を使用して、単一の構成変更を展開することも、待機して複数の変更を一度に展開することもできます。

手順の概要

1. 画面の右上隅で [展開] アイコン をクリックします。
2. 展開する変更があるデバイスを選択します。デバイスに黄色の三角の注意マークが付いている場合、そのデバイスに変更を展開することはできません。黄色の三角の注意マークにマウスを合わせると、そのデバイスに変更を展開できない理由を確認できます。
3. デバイスを選択したら、右側のパネルでデバイスを拡大し、具体的な変更をプレビューできます。
4. （オプション）保留中の変更に関する詳細情報を表示する場合は、[詳細な変更ログを表示] リンクをクリックして、その変更に関連付けられた変更ログを開きます。[展開] アイコンをクリックして、[保留中の変更があるデバイス] ページに戻ります。
5. （オプション）[保留中の変更があるデバイス] ページを離れずに、変更を追跡する変更リクエストを作成します。
6. [今すぐ展開] をクリックして、選択したデバイスに今すぐ変更を展開します。[ジョブ] トレイの [アクティブなジョブ] インジケータに進行状況が表示されます。

7. （オプション）展開が完了したら、CDO ナビゲーションバーの [ジョブ] をクリックします。展開の結果を示す最近の「変更の展開」ジョブが表示されます。
8. 変更リクエストラベルを作成し、それに関連付ける構成変更がない場合は、それをクリアします。

手順の詳細

ステップ 1 画面の右上隅で [展開] アイコン をクリックします。

ステップ 2 展開する変更があるデバイスを選択します。デバイスに黄色の三角の注意マークが付いている場合、そのデバイスに変更を展開することはできません。黄色の三角の注意マークにマウスを合わせると、そのデバイスに変更を展開できない理由を確認できます。

ステップ 3 デバイスを選択したら、右側のパネルでデバイスを拡大し、具体的な変更をプレビューできます。

ステップ 4 （オプション）保留中の変更に関する詳細情報を表示する場合は、[詳細な変更ログを表示] リンクをクリックして、その変更に関連付けられた変更ログを開きます。[展開] アイコンをクリックして、[保留中の変更があるデバイス] ページに戻ります。

ステップ 5 （オプション）[保留中の変更があるデバイス] ページを離れずに、変更を追跡する変更リクエストを作成します。

ステップ 6 [今すぐ展開] をクリックして、選択したデバイスに今すぐ変更を展開します。[ジョブ] トレイの [アクティブなジョブ] インジケータに進行状況が表示されます。

ステップ 7 （オプション）展開が完了したら、CDO ナビゲーションバーの [ジョブ] をクリックします。展開の結果を示す最近の「変更の展開」ジョブが表示されます。

ステップ 8 変更リクエストラベルを作成し、それに関連付ける構成変更がない場合は、それをクリアします。

次のタスク

- スケジュールされた自動展開
- CDO から ASA に設定変更を展開します。 （179 ページ）
- ASA に展開後の変更ログエントリ

CDO から ASA に設定変更を展開します。

CDO が ASA に変更を展開する理由

Cisco Defense Orchestrator（CDO）を使用してデバイスの設定を管理および変更すると、加えた変更が CDO により構成ファイルの独自のコピーに保存されます。これらの変更は、デバイスに「展開」されるまで、CDO で「ステージング」されたと見なされます。ステージングされた設定変更は、デバイスを通過するネットワークトラフィックには影響しません。CDO がデバイスに変更を「展開」した後にのみ、デバイスを通過するトラフィックに影響を与えます。

CDO がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体を上書きすることはありません。

ASA には、「実行構成」とも呼ばれる「実行」構成ファイルと、「スタートアップ コンフィギュレーション」とも呼ばれる「起動」構成ファイルがあります。実行コンフィグレーションファイルに保存されている構成は、ASA を通過するトラフィックに適用されます。実行コンフィグレーションに変更を加え、それらの変更がもたらす動作に問題がないことを確認したら、それらをスタートアップ コンフィギュレーションに展開できます。ASA が再起動されるたびに、スタートアップコンフィギュレーションが構成の開始点として使用されます。実行コンフィギュレーシに加えた変更で、スタートアップコンフィギュレーションに保存されていないものは、ASA の再起動後にすべて失われます。

CDO から ASA に変更を展開すると、それらの変更が実行構成ファイルに書き込まれます。これらの変更によってもたらされる動作に問題がなければ、それらの変更をスタートアップ コンフィギュレーション ファイルに展開できます。

展開は、1 つのデバイスに対して開始することも、複数のデバイスに対して同時に開始することもできます。単一のデバイスに対して、個別の展開や繰り返しの展開をスケジュールできます。

一部の変更は ASA に直接展開される

CDO で CLI インターフェイス CLI マクロを使用して ASA に変更を加えた場合、それらの変更は CDO で「ステージング」されません。それらは、ASA の実行構成に直接展開されます。このように変更を加えると、デバイスは CDO と「同期」状態が維持されます。

設定変更の展開について

このセクションでは、ASA 構成ファイルを変更するために、CDO の CLI インターフェイスまたは CLI マクロインターフェイスを使用せずに、CDO の GUI を使用しているか、[デバイス設定（Device Configuration）] ページを編集していることを前提としています。

ASA 設定の更新は、2 段階のプロセスです。

ステップ 1 次のいずれかの方法を使用して、CDO で変更を加えます。

- CDO GUI
- [デバイス設定（Device Configuration）] ページのデバイス設定

ステップ 2 変更を加えたら、[デバイスとサービス] ページに戻り、[プレビューと展開（Preview and Deploy...）] でデバイスへの変更をプレビューして展開します。

次のタスク

CDO が ASA の実行構成を CDO でステージングされた設定で更新する場合、または ASA に保存されている実行構成で CDO 上の設定を変更する場合、CDO は、設定の変更部分が CDO GUI

で管理可能な場合、構成ファイルの関連する行のみを変更しようとします。CDO GUI を使用して目的の構成変更を行うことができない場合、CDO は構成ファイル全体を上書きして変更を加えようとします。

2 つの例を示します。

- ネットワークオブジェクトは、CDO GUI を使用して作成または変更が可能です。CDO がその変更を ASA の設定に展開する必要がある場合、変更が発生したときに ASA の実行構成ファイルの関連する行が上書きされます。
- 新しいローカル ASA ユーザーは CDO GUI を使用して作成することはできませんが、[デバイスの設定（Device Configuration）] ページで ASA の設定を編集することで作成できます。[デバイスの設定（Device Configuration）] ページでユーザーを追加し、その変更を ASA に展開すると、CDO は実行構成ファイル全体を上書きして、その変更を ASA の実行構成ファイルに保存しようとします。

CDO GUIを使用して行った設定変更の展開

ステップ 1 CDO GUI を使用して構成を変更し、変更を保存すると、その変更は CDO に保存されたバージョンの ASA の実行構成ファイルに保存されます。

ステップ 2 [デバイスとサービス] ページでデバイスに戻ります。

ステップ 3 [デバイス]_タブをクリックします。デバイスが「未同期」になっていることがわかります。

ステップ 4 次のいずれかの方法を使用して、変更を展開します。

- 画面右上の [展開（Deploy）] アイコン をクリックします。これにより、デバイスに加えた変更を展開する前に確認することができます。変更を加えたデバイスを確認し、デバイスを展開して変更を確認し、[今すぐ展開（Deploy Now）] をクリックして変更を展開します。

  （注） [保留中の変更があるデバイス] 画面でデバイスの横に黄色の警告三角形が表示されている場合、変更を展開することはできません。警告の三角形にマウスを合わせると、デバイスに変更を展開できない理由が表示されます。

- [未同期（Not Synced）] ウィンドウで、[プレビューして展開...（Preview and Deploy...）] をクリックします。

  1. ASA コンフィギュレーション ファイルを変更するコマンドを確認します。
  2. コマンドに問題がない場合は、[リカバリプリファレンスの設定（Configuration Recovery Preference）] を選択します。

     （注） [通知を受け取り、設定を手動で復元します。（Let me know and I will restore the configuration manually）] を選択した場合、続行する前に、[手動同期手順の表示（View Manual Synchronization Instructions）] をクリックします。

  3. [デバイスに変更を適用する（Apply Changes to Device）] をクリックします。

4. [OK] をクリックして成功メッセージを確認します。

自動展開をスケジュール設定する

自動展開のスケジュールことにより、単一のデバイスまたは保留中の変更があるすべてのデバイスへの展開をスケジュールするようにテナントを設定することもできます。

CDO の CLI インターフェイスを使用した設定変更の展開

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 設定を編集するデバイスを選択します。

ステップ 5 [アクション] ペインで、[>_コマンド ライン インターフェイス（>_Command Line Interface）] をクリックします。

ステップ 6 コマンド ライン インターフェイス テーブルにコマンドがある場合は、[クリア] をクリックしてそれらを削除します。

ステップ 7 コマンドラインインターフェイスの表の上部のボックスにあるコマンドプロンプトに、コマンドを入力します。各コマンドを個別の行に入力するか、構成ファイルのセクションをコマンドとして入力することにより、1 つのコマンドを実行したり、複数のコマンドを一括で実行したりできます。コマンド ライン インターフェイス テーブルに入力できるコマンドの例を次に示します。

ネットワークオブジェクト「albany」を作成する単一のコマンド

```
object network albany
host 209.165.30.2
```

一緒に送信される複数のコマンド：

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

コマンドとして入力された実行構成ファイルのセクション：

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

（注） CDO では、EXEC モード、特権 EXEC モード、およびグローバル コンフィギュレーション モードの間を移動する必要はありません。入力したコマンドは適切なコンテキストで解釈されます。

ステップ 8 コマンドを入力したら、[送信（Send）] をクリックします。CDO が ASA の実行中の構成ファイルへの変更を正常に展開すると、[完了（Done!）] というメッセージが表示されます。

ステップ 9 コマンドを送信した後で、「一部のコマンドが実行構成に変更を加えた可能性があります」というメッセージが 2 つのリンクとともに表示されることがあります。

- [ディスクに展開（Deploy to Disk）] をクリックすると、このコマンドによって加えられた変更と、実行構成のその他の変更が、ASA のスタートアップ構成に保存されます。
- [取り消す（Dismiss）] をクリックすると、メッセージが取り消されます。

デバイス設定の編集による設定変更の展開

注意 この手順は、ASA 設定ファイルの構文に精通している上級ユーザーを対象としています。この手法では、CDO に保存されている実行設定ファイルに直接変更を加えます。

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 設定を編集するデバイスを選択します。

ステップ 5 [アクション] ペインで、[設定の表示（View Configuration）] をクリックします。

ステップ 6 [編集（Edit）] をクリックします。

ステップ 7 実行中の設定に変更を加えて**保存**します。

ステップ 8 [デバイスとサービス（Devices & Services）] ページに戻ります。[未同期（Not Synced）] ウィンドウで、[プレビューして展開...（Preview and Deploy...）] をクリックします。

ステップ 9 [デバイスの同期（Device Sync）] ウィンドウで、変更を確認します。

ステップ 10 変更の種類に応じて、[変更の置換（Replace Configuration）] または [変更のデバイスへの適用（Apply Changes to Device）] をクリックします。

複数デバイス上の共有オブジェクトの設定変更の展開

この手順は、2 つ以上のデバイスで共有されているポリシーまたはオブジェクトに変更を加える場合に使用します。多くのデバイスで使用されている共通ポリシーを変更できます。

ステップ 1 編集する共有オブジェクトを含む [ポリシー（Policies）] ページまたは [オブジェクト] ページを開いて編集します。

ステップ 2 共有デバイスリストを確認し、挙げられているすべてのデバイスに変更を加えることを確認します。

ステップ 3 [確認（Confirm）] をクリックします。

ステップ 4 [**保存**（**Save**）] をクリックします。

ステップ 5 [展開] アイコンをクリックして、すべてのデバイスの構成変更のプレビューと展開します。

デバイス設定の一括展開

共有オブジェクトを編集するなどして複数のデバイスに変更を加えた場合、影響を受けるすべてのデバイスにそれらの変更を一度に適用できます。

ステップ 1 ナビゲーションウィンドウで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 CDO で設定を変更した、すべてのデバイスを選択します。これらのデバイスは、「未同期」ステータスが表示されているはずです。

ステップ 5 次のいずれかの方法を使用して、変更を展開します。

- 画面右上の [展開] ボタン をクリックします。これにより、選択したデバイス上の保留中の変更を展開する前に確認することができます。変更を展開するには、[今すぐ展開（Deploy Now）] をクリックします。

  （注） [保留中の変更があるデバイス] 画面でデバイスの横に黄色の警告三角形が表示されている場合、そのデバイスに変更を展開することはできません。そのデバイスに変更を展開できない理由を確認するには、警告三角形の上にマウスカーソルを置きます。

- 詳細ペインで [すべて展開（Deploy All）] をクリックします。すべての警告を確認し、[OK] をクリックします。一括展開は、変更を確認せずにすぐに開始します。

ステップ 6 （任意）ナビゲーションバーの [ジョブ] アイコン をクリックして、一括展開の結果を表示します。

関連情報：

- 自動展開のスケジュール （185 ページ）

スケジュールされた自動展開

CDO を使用すると、CDO が管理する 1 つ以上のデバイスの構成を変更し、都合のよいタイミングでそれらのデバイスに変更を展開するようにスケジュールできます。

[設定] ページの [テナント設定] タブで 自動展開をスケジュールするオプションを有効にする をした場合のみ、展開をスケジュールできます。このオプションを有効にすると、展開スケジュールを作成、編集、削除できます。展開スケジュールによって、CDO に保存されたすべてのステージング済みの変更が、設定した日時に展開されます。[ジョブ]ページから、展開スケジュールを表示および削除することもできます。

CDOに変更の読み取り、破棄、チェック、および展開変更がデバイスに直接加えられた場合、その競合が解決されるまで、展開スケジュールはスキップされます。[ジョブ]ページには、スケジュールされた展開が失敗したインスタンスが一覧表示されます。[自動展開をスケジュールするオプションを有効にする] をオフにすると、スケジュールされたすべての展開が削除されます。

注意 複数のデバイスの新しい展開をスケジュールし、それらのデバイスの一部に展開が既にスケジュールされている場合、既存の展開スケジュールが新しい展開スケジュールで上書きされます。

（注） 展開スケジュールを作成すると、スケジュールはデバイスのタイムゾーンではなく現地時間で作成されます。展開スケジュールは、サマータイムに合わせて自動的に調整されません。

自動展開のスケジュール

展開スケジュールは、単一のイベントまたは繰り返し行われるイベントにすることができます。繰り返し行われる自動展開は、繰り返し行われる展開をメンテナンス期間に合わせるための便利な方法です。次の手順に従って、単一のデバイスに対して1回限りまたは繰り返し行われる展開をスケジュールします。

（注） 既存の展開がスケジュールされているデバイスへの展開をスケジュールすると、新しくスケジュールされた展開によって既存の展開が上書きされます。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 1 つ以上のデバイスを選択します。

ステップ 5 [デバイスの詳細] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[スケジュール（Schedule）] をクリックします。

ステップ 6 展開をいつ実行するかを選択します。

- 1 回限りの展開の場合は、[1回限り（Once on）] オプションをクリックして、カレンダーから日付と時刻を選択します。
- 繰り返し展開する場合は、[定期（Every）] オプションをクリックします。日に 1 回と週に 1 回のいずれかの展開を選択できます。展開を実行する [曜日（Day）] と [時刻（Time）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の編集

スケジュールされた展開を編集するには、次の手順に従います。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
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 1 つ以上のデバイスを選択します。
ステップ 5 [デバイスの詳細] ペインで、[スケジュールされた展開（Scheduled Deployments）] タブを見つけて、[編集] をクリックします。

ステップ 6 スケジュールされた展開の繰り返し回数、日付、または時刻を編集します。
ステップ 7 [保存（Save）] をクリックします。

スケジュールされた展開の削除

スケジュールされた展開を削除するには、次の手順に従います。

（注） 複数のデバイスの展開をスケジュールしてから、一部のデバイスのスケジュールを変更または削除した場合は、残りのデバイスの元のスケジュールされた展開が保持されます。

ステップ 1 ナビゲーションバーで、[デバイスとサービス] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
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 1 つ以上のデバイスを選択します。

ステップ 5 [デバイスの詳細] ペインで、[スケジュールされた展開（ Scheduled Deployments）] タブを見つけて、[削除（Delete）] をクリックします。

次のタスク

- 変更の読み取り、破棄、チェック、および展開
- すべてのデバイス設定の読み取り （176 ページ）
- CDO から ASA に設定変更を展開します。 （179 ページ）
- すべてのデバイスの構成変更のプレビューと展開 （178 ページ）

設定変更の確認

[変更の確認（Check for Changes）] をクリックして、デバイスの設定がデバイス上で直接変更されているか、CDO に保存されている設定のコピーと異なっているかどうかを確認します。このオプションは、デバイスが [同期（Synced）] 状態のときに表示されます。

変更を確認するには、次の手順を実行します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。
ステップ 2 [デバイス] タブをクリックします。
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 設定がデバイス上で直接変更された可能性があるデバイスを選択します。
ステップ 5 右側の [同期（Synced）] ペインで [変更の確認（Check for Changes）] をクリックします。
ステップ 6 次の動作は、デバイスによって若干異なります。

- デバイスの場合、デバイスの設定に変更があった場合、次のメッセージが表示されます。

```
Reading the policy from the device. If there are active deployments on the device, reading will start after they are finished.
```

  - [OK] をクリックして、先へ進みます。デバイスの設定で、CDO に保存されている設定が上書きされます。
  - 操作をキャンセルするには、[キャンセル] をクリックします。

- ASA デバイスの場合：

1. 提示された 2 つの設定を比較します。[続行（Continue）] をクリックします。**最後に認識されたデバイス設定（Last Known Device Configuration）**というラベルの付いた設定は、CDO に保存されている設定です。**デバイスで検出（Found on Device）**というラベルの付いた設定は、ASA に保存されている設定です。

2. 次のいずれかを選択します。
    1. [拒否（Reject）] : アウトオブバンド変更を拒否して、「最後に認識されたデバイス設定（Last Known Device Configuration）」を維持します。
    2. [承認（Accept）] : アウトオブバンド変更を承認して、CDO に保存されているデバイスの設定を、デバイスで見つかった設定で上書きします。
3. [続行（Continue）] をクリックします。

変更の破棄

CDO を使用してデバイスの構成に加えた、展開されていない構成変更のすべてを「元に戻す」場合は、[変更の破棄（Discard Changes）] をクリックします。[変更の破棄（Discard Changes）] をクリックすると、CDO は、デバイスに保存されている構成でデバイスの構成のローカルコピーを完全に上書きします。

[変更の破棄（Discard Changes）] をクリックすると、デバイスの構成ステータスは [非同期] 状態になります。変更を破棄すると、CDO 上の構成のコピーは、デバイス上の構成のコピーと同じになり、CDO の構成ステータスは [同期済み] に戻ります。

デバイスの展開されていない構成変更のすべてを破棄する（つまり「元に戻す」）には、次の手順を実行します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

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 構成変更を実行中のデバイスを選択します。

ステップ 5 右側の [非同期] ペインで [変更の破棄（Discard Changes）] をクリックします。

- FTD デバイスの場合は、「Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device（CDO 上の保留中の変更は破棄され、このデバイスに関する CDO 構成は、デバイス上の現在実行中の構成に置き換えられます）」という警告メッセージが表示されます。[続行] をクリックして変更を破棄します。
- Meraki デバイスの場合は、変更がすぐに削除されます。
- AWS デバイスの場合は、削除しようとしているものが表示されます。[同意する（Accept）] または [キャンセル] をクリックします。

デバイスのアウトオブバンド変更

アウトオブバンド変更とは、CDO を使用せずにデバイス上で直接行われた変更を指します。アウトオブバンド変更は、SSH 接続を介してデバイスのコマンドライン インターフェイスを使用して、または、ASA の場合は Adaptive Security Device Manager（ASDM）、FTD の場合は FDM などのローカルマネージャを使用して行うことができます。アウトオブバンド変更により、CDO に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

デバイスでのアウトオブバンド変更の検出

ASA、FTD、または Cisco IOS デバイスに対して競合検出が有効になっている場合、CDO は 10 分ごとにデバイスをチェックし、CDO の外部でデバイスの設定に直接加えられた新たな変更を検索します。

CDO は、CDO に保存されていないデバイスの設定に対する変更を検出した場合、そのデバイスの [設定ステータス（Configuration Status）] を [競合検出（Conflict Detected）] 状態に変更します。

Defense Orchestrator が競合を検出した場合、次の 2 つの状態が考えられます。

- CDO のデータベースに保存されていない設定変更が、デバイスに直接加えられています。
- FTD の場合、展開されていない「保留中」の設定変更がある可能性があります。

Defense Orchestrator とデバイス間の設定を同期する

設定の競合について

[デバイスとサービス]ページで、デバイスまたはサービスのステータスが [同期済み]、[未同期（Not Synced）]、または [競合が検出されました（Conflict Detected）] になっていることがあります。

- デバイスが [同期済み] の場合、Cisco Defense Orchestrator（CDO）の設定と、デバイスにローカルに保存されている設定は同じです。
- デバイスが [未同期（Not Synced）] の場合、CDO に保存された設定が変更され、デバイスにローカルに保存されている設定とは異なっています。CDO からデバイスに変更を展開すると、CDO のバージョンに一致するようにデバイスの設定が変更されます。
- CDO の外部でデバイスに加えられた変更は、**アウトオブバンドの変更**と呼ばれます。デバイスの競合検出が有効になっている場合、アウトオブバンドの変更が行われると、デバイスのステータスが [競合が検出されました（Conflict Detected）] に変わります。アウトオブバンドの変更を受け入れると、CDO の設定がデバイスの設定と一致するように変更されます。

競合検出

競合検出が有効になっている場合、Cisco Defense Orchestrator（CDO）はデフォルトの間隔でデバイスをポーリングして、CDO の外部でデバイスの構成が変更されたかどうかを判断します。変更が行われたことを検出すると、CDO はデバイスの構成ステータスを [競合が検出されました] に変更します。CDO の外部でデバイスに加えられた変更は、「アウトオブバンド」の変更と呼ばれます。

このオプションを有効にすると、デバイスごとに競合または OOB 変更を検出する頻度を設定できます。詳細については、デバイス変更のポーリングのスケジュール（193 ページ）を参照してください。

競合検出の有効化

競合検出を有効にすると、Defense Orchestrator の外部でデバイスに変更が加えられた場合に警告が表示されます。

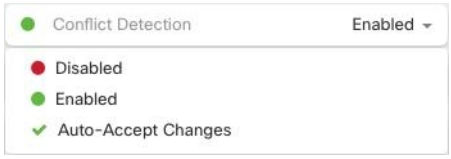
ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 適切なデバイスタイプのタブを選択します。

ステップ 4 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 デバイステーブルの右側にある [競合検出] ボックスで、リストから [有効（Enabled）] を選択します。



デバイスからのアウトオブバンド変更の自動的な受け入れ

変更の自動的な受け入れを有効にすることで、管理対象デバイスに直接加えられた変更を自動的に受け入れるように Cisco Defense Orchestrator（CDO）を設定できます。CDO を使用せずにデバイスに直接加えられた変更は、アウトオブバンド変更と呼ばれます。アウトオブバンドの変更により、CDO に保存されているデバイスの設定とデバイス自体に保存されている設定との間で競合が発生します。

変更の自動受け入れ機能は、競合検出のための強化機能です。デバイスで変更の自動受け入れを有効にしている場合、CDO は 10 分ごとに変更をチェックして、デバイスの設定に対してア

ウトオブバンドの変更が行われたかどうかを確認します。設定が変更されていた場合、CDO は、プロンプトを表示することなく、デバイスの設定のローカルバージョンを自動的に更新します。

CDO で行われたいずれかの設定変更がデバイスにまだ展開されていない場合、CDO は設定変更を自動的に**受け入れません**。画面上のプロンプトに従って、次のアクションを決定します。

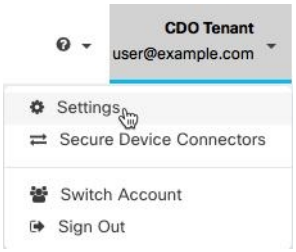
変更の自動受け入れを使用するには、最初に、テナントが [デバイスとサービス] ページの [競合検出] メニューで自動受け入れオプションを表示できるようにします。次に、個々のデバイスでの変更の自動受け入れを有効にします。

CDO でアウトオブバンドの変更を検出するものの、変更を手動で受け入れたり拒否したりするオプションを選択する場合は、代わりに 競合検出 （190 ページ） を有効にします。

自動承認変更の設定

ステップ 1 管理者またはネットワーク管理者権限を持つアカウントを使用して CDO にログインします。

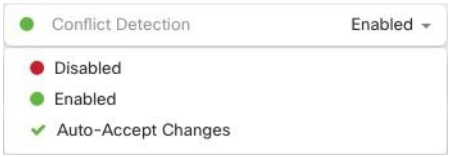
ステップ 2 ユーザーメニューから [設定] をクリックして、[設定] ページにアクセスします。



ステップ 3 [テナント設定] エリアで、[デバイスの変更を自動承認するオプションの有効化] のトグルをクリックします。これにより、[デバイスとサービス] ページの [競合検出] メニューに [変更の自動承認] メニューオプションが表示されるようになります。

ステップ 4 [デバイスとサービス] ページを開き、アウトオブバンドの変更を自動承認するデバイスを選択します。

ステップ 5 [競合検出] メニューで、ドロップダウンメニューから [変更の自動承認] を選択します。



テナント上のすべてのデバイスの自動承認変更の無効化

ステップ 1 管理者またはスーパー管理者権限を持つアカウントを使用して CDO にログインします。

ステップ 2 ユーザーメニューから [設定] をクリックして、[設定] ページにアクセスします。

ステップ 3 [テナント設定] 領域で、トグルを左にスライドして灰色の X を表示し、[デバイスの変更を自動承認するオプションを有効にする（Enable the option to auto-accept device changes）] を無効にします。これにより、競合検出メニューの [変更の自動承認] オプションが無効になり、テナント上のすべてのデバイスでこの機能が無効になります。

（注） [自動承認（Auto-Accept）] を無効にした場合、CDO で承認する前に、各デバイスの競合を確認する必要があります。これまで変更の自動承認が設定されていたデバイスも対象になります。

設定の競合の解決

このセクションでは、デバイスで発生する設定の競合の解決に関する情報を提供します。

「未同期」ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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 未同期と報告されたデバイスを選択します。

ステップ 5 右側の [未同期（Not synced）] パネルで、次のいずれかを選択します。

- [プレビューして展開...（Preview and Deploy..）]：設定の変更を CDO からデバイスにプッシュする場合は、今行った変更をすべてのデバイスの構成変更のプレビューと展開か、待ってから一度に複数の変更を展開します。
- [変更の破棄（Discard Changes）]：設定の変更を CDO からデバイスにプッシュ**したくない**場合、または CDO で開始した設定の変更を「元に戻す」場合。このオプションは、CDO に保存されている設定を、デバイスに保存されている実行中の設定で上書きします。

[競合検出（Conflict Detected）] ステータスの解決

CDO を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。競合検出 （190 ページ） が有効になっていて、CDO を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出（Conflict Detected）] と表示されます。

[競合検出（Conflict Detected）] ステータスを解決するには、次の手順に従います。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] をクリックします。

ステップ 2 [デバイス] タブをクリックして、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 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認（Review Conflict）] をクリックします。

ステップ 5 [デバイスの同期（Device Sync）] ページで、強調表示されている相違点を確認して、2 つの設定を比較します。

- 「最後に認識されたデバイス設定（Last Known Device Configuration）」というラベルの付いたパネルは、CDO に保存されているデバイス設定です。
- 「デバイスで検出（Found on Device）」というラベルの付いたパネルは、ASA の実行構成に保存されている設定です。

ステップ 6 次のいずれかを選択して、競合を解決します。

- [デバイスの変更を承認（Accept Device changes）]：設定と、CDO に保存されている保留中の変更がデバイスの実行構成で上書きされます。

  （注） CDO はコマンド ライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認（Accept Without Review）] です。

- [デバイスの変更を拒否（Reject Device Changes）]：デバイスに保存されている設定を CDO に保存されている設定で上書きします。

（注） 拒否または承認されたすべての設定変更は、変更ログに記録されます。

デバイス変更のポーリングのスケジュール

競合検出 （190 ページ） を有効にしている場合、または [設定] ページで [デバイスの変更を自動承認するオプションの有効化] オプションを有効にしている場合、CDO はデフォルトの間隔でデバイスをポーリングして、CDO の外部でデバイスの設定に変更が加えられたかどうかを判断します。CDO による変更のポーリング間隔は、デバイスごとにカスタマイズできます。ポーリング間隔の変更は、複数のデバイスに適用できます。

デバイスでこの間隔が選択されていない場合は、間隔は「テナントのデフォルト」に自動的に設定されます。

（注） [デバイスとサービス]ページでデバイスごとの間隔をカスタマイズすると、[全般設定（General Settings）] ページの [デフォルトの競合検出間隔（Default Conflict Detection Interval）]デフォルトの競合検出間隔で選択したポーリング間隔が上書きされます。

[デバイスとサービス（Conflict Detection）] ページで [競合検出] を有効にするか、[設定] ページで[デバイスの変更を自動承認するオプションの有効化]オプションを有効にしたら、次の手順に従い CDO によるデバイスのポーリング間隔をスケジュールします。

ステップ 1 ナビゲーションバーで、[デバイスとサービス（Devices & Services）] 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 競合検出を有効にする 1 台または複数のデバイスを選択します。

ステップ 5 [競合検出] と同じ領域で、[チェック間隔（Check every）] のドロップダウンメニューをクリックし、目的のポーリング間隔を選択します。