ポリシーの設定

ポリシーの概要

Cisco DNA Center を使用すると、ネットワークの特定の側面（ネットワークアクセスなど）に対する組織のビジネス目標を反映したポリシーを作成できます。Cisco DNA Center は、ポリシー内で収集された情報を取得し、お使いのネットワークデバイスのさまざまなタイプ、メーカー、モデル、オペレーティングシステム、ロール、およびリソースの制約によって必要とされる、ネットワーク固有およびデバイス固有の設定に変換します。

Cisco DNA Center を使用して、仮想ネットワーク、アクセス コントロール ポリシー、トラフィック コピー ポリシー、およびアプリケーション ポリシーを作成できます。

グループベースのアクセス コントロール ポリシー

Cisco DNA Center は、次の 2 つの方法で Software-Defined Access を実装します。

- 仮想ネットワーク（VN）は、たとえば、企業のネットワークから IoT デバイスを分離するといった、マクロレベルのセグメンテーションを提供します。
- グループベースのポリシーは、たとえば、エンジニアリンググループと HR グループの間で許可または拒否するネットワークトラフィックのタイプを制御するといった、マイクロレベルのセグメンテーションを提供します。

グループベースのアクセス コントロール ポリシー メニューを使用すると、スケーラブルなグループアクセスポリシーを監視および管理できます。それらのポリシーには、次の利点があります。

- ネットワークの自動化とアシュアランスの利点を備えた、豊富なアイデンティティベースのアクセス制御機能。
- きめ細かいアクセス制御。
- スケーラブルグループは、すべての仮想ネットワークに適用されるため、ポリシー管理が簡素化されます。
- ポリシービューは、全体的なポリシー構造を理解し、必要なアクセス コントロール ポリシーを作成または更新するのに役立ちます。
- さまざまなアプリケーションを切り替えてスケーラブルグループを管理し、保護される資産を定義する必要がなくなります。
- エンタープライズ全体のアクセス コントロール ポリシーを展開するための拡張機能を提供します。
- アイデンティティまたはネットワーク アドミッション コントロール（NAC）アプリケーションが配置される前に、ランサムウェアなどの脅威のラテラルムーブメントを制限します。
- サードパーティのアイデンティティ アプリケーションを使用しているが、Cisco ISE に移行したいユーザーに対して、Cisco Identity Services Engine（Cisco ISE）への簡単な移行パスを提供します。

Cisco DNA Center での IP プール、サイト、および仮想ネットワークの作成方法については、Cisco DNA Center のユーザーガイドを参照してください。

Cisco DNA Center for Cisco ISE の設定の詳細については、Cisco DNA Center のインストールガイドを参照してください。

Cisco ISE for Cisco DNA Center の設定の詳細については、Cisco Identity Services Engine 管理者ガイド [英語] を参照してください。

まず、スケーラブルなグループと契約を定義してから、アクセス コントロール ポリシーを作成します。アクセス コントロール ポリシーは、送信元スケーラブルグループから宛先スケーラブルグループに渡すことができるネットワークトラフィックを定義します。

- **スケーラブルグループ**：ユーザー、ネットワークデバイス、またはリソースを割り当てることができる分類カテゴリ。スケーラブルグループは、アクセス コントロール ポリシーで使用されます。組織のネットワーク設定、アクセス要件、および制限に基づいて、スケーラブルグループを仮想ネットワークに関連付けることができます。
- **契約**：アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。つまり、契約はトラフィックフィルタの定義です。アクセス契約は、トラフィックがネットワーク アプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒

否）を定義します。他のルールが一致しない場合、デフォルトアクションでは Catch All ルールが使用されます。

- **グループベースのアクセス コントロール ポリシー**：グループベースのアクセス コントロール ポリシーは、特定の送信元と宛先グループのペアを識別し、アクセス契約を関連付けます。アクセス契約は、送信元グループと宛先グループの間で許可または拒否されるトラフィックのタイプを指定します。これらのポリシーは単方向です。

  スケーラブルグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセス コントロール ポリシーを作成する際には、前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作成したりできます。特定の送信元グループからアクセスできるネットワーク リソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。一方、特定のネットワーク リソースへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザーがアクセスできるネットワーク リソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。「財務サーバー」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

  送信元と宛先のスケーラブルグループの組み合わせにコントラクトが指定されていない場合に使用するデフォルトポリシーを指定できます。デフォルトポリシーは [Permit] です。必要に応じて、このポリシーを [Deny]、[Permit_IP_Log]、または [Deny_IP_Log] に変更できます。ネットワークタイプ、オープンネットワーク、またはクローズドネットワークに基づいて、デフォルトポリシーを設定できます。

（注） すべてのネットワーク インフラストラクチャ デバイスに必要なネットワークトラフィックを許可する明示的なポリシーを作成した場合のみ、デフォルトポリシーを [Permit] から [Deny] に変更することをお勧めします。そのようにしない場合、すべてのネットワーク接続が失われる可能性があります。

リスト ビュー

[Group-Based Access Control] ウィンドウの右上にある [List] アイコンをクリックして、[List] ビューを起動します。

- [Source View]：送信元グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。
- [Destination View]：宛先グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。

特定の送信元グループから使用可能な宛先グループを確認するには、[Source] ビューを使用します。特定の宛先グループへのアクセスが許可されている送信元グループを確認するには、[Destination] ビューを使用します。たとえば、「請負業者」送信元スケーラブルグループの一部であるユーザーが使用できる宛先グループを確認するには、[Source] ビューを使用します。「財務サーバー」宛先スケーラブルグループにアクセスできる送信元グループを確認するには、[Destination] ビューを使用します。

ポリシー適用統計データをポリシーリストテーブルで表示することもできます。選択した期間内のポリシーの許可と拒否の総数が表示されます。

ポリシー適用統計は、グループベースのポリシーおよびテレメトリデータ言語（TDL）サブスクリプション用にプロビジョニングされたネットワークデバイスから収集されます。これらの設定は、通常、ファブリックの一部であるネットワークデバイスに関して自動的にプロビジョニングされます。非ファブリック ネットワーク デバイスに関しては手動設定を実行できます。

ポリシー適用統計データを使用する場合は、次の点に注意してください。

- ポリシー適用統計データは、グループベースポリシー分析パッケージが展開されている場合にのみ使用できます。
- テレメトリ サブスクリプションは、ファブリック ネットワーク デバイスと非ファブリック ネットワーク デバイスの両方に関する基本プロビジョニングの一部として追加されます。新しいネットワークデバイスが DNAC に追加され、サイトに割り当てられると、TrustSec 適用コマンドがプッシュされます。
- Software-Defined Access（SDA）は、ファブリックに追加されたネットワークデバイスに TrustSec 適用を追加します。TrustSec テレメトリデータは、ネットワークデバイスでこの適用が有効になっている場合にのみ収集されます。有効になっていない場合は、ポリシーモニターリングに使用されるテレメトリ サブスクリプションが TrustSec の TDL データの収集に使用されます。
- Cisco IOS XE 16.12 以降では、TDL ストリーミングデータがサポートされています。
- ネットワークデバイスで NETCONF を有効にする必要があります。
- 非ファブリック ネットワーク デバイスについては、次の設定を手動で追加する必要があります。

  ```
  cts role-based enforcement vlan-list <VLAN of the endpoints>
  ```

- Cisco DNA Center 2.2.2 にアップグレードすると、[Provision] > [Network Devices] > [Inventory] ウィンドウに次のメッセージが表示される場合があります。

  IOS-XE デバイスがネットワークで検出されました。これには、保証データの新しいテレメトリ サブスクリプションを有効にし、既存のサブスクリプションの一部をパフォーマンスのために最適化する必要があります。netconf を有効にし、これらのデバイスのインベントリクレデンシャルで netconf ポートを設定する必要があることに注意してください。また、これらのデバイスは、グループベースのポリシー モニターリング テレメトリの新しいサブスクリプションを受信することに注意してください。これらのサブスクリプションをプロビジョニングするためのアクションを実行しますか?

  [Apply Fix] をクリックして、サイトが割り当てられているすべてのネットワークデバイスに設定をプッシュします。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco Identity Services Engine（Cisco ISE）に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

マトリクス ビュー

[Group-Based Access Control] ウィンドウの右上にある [Grid] アイコンをクリックして、[Matrix] ビューを起動します。[Matrix] ビューはコアポリシービューであり、すべてのスケーラブルグループに関するすべてのポリシーの概要を提供します（明示的またはデフォルトを問わない）。[Matrix] ビューを使用して、すべての送信元と宛先のポリシーを表示し、全体的なポリシー構造を理解できます。[Matrix] ビューからアクセス コントロール ポリシーを表示、作成、および更新できます。

[Matrix] ビューには、次の 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元スケーラブルグループがリストされます。
- 宛先軸：水平軸にはすべての宛先スケーラブルグループがリストされます。

特定の送信元スケーラブルグループと宛先スケーラブルグループのポリシーを表示するには、セルにカーソルを置きます。セルの色は、そのセルに適用されるポリシーに基づいています。次の色は、各セルに適用されるポリシーを示しています。

- [Permit]：緑色
- [Deny]：赤色
- [Custom]：金色
- [Default]：灰色

マトリックスの上部に表示される [Permit]、[Deny]、[Custom]、または [Default] アイコンにカーソルを置くと、そのポリシーが適用されているセルが表示されます。

セルをクリックすると、[Create Plicy] または [Edit Policy] スライドインペインが開き、選択したセルのポリシーを作成または編集できます。[Create Policy] スライドインペインには、送信元と宛先のスケーラブルグループが読み取り専用フィールドとして表示されます。ポリシーのステータスとアクセス契約を更新できます。

ポリシーマトリックスのカスタムビューを作成して、関心のあるポリシーだけに絞り込むことができます。これを実行するには、[View] ドロップダウンリストをクリックし、[Create View] を選択します。カスタムビューを作成するときに、カスタムビューに含めるスケーラブルグループのサブセットを指定できます。必要に応じて、カスタムビューを保存し、後で編集することができます。[View] ドロップダウンリストをクリックし、[Manage Views] を選択して、カスタムビューを作成、編集、複製、または削除します。[Default View] には、すべての送信元および宛先スケーラブルグループが表示されます。

カーソルでマトリックスコンテンツ領域をドラッグするか、または水平および垂直スクロールバーを使用して、マトリックス内を移動できます。ミニマップを使用して、マトリックス内を移動することもできます。ミニマップを使用すると、マトリックスのサイズが大きく、画面サイズを超えている場合に、マトリックス内を簡単に移動できます。ミニマップは、画面上の任

意の場所に移動して配置できます。ミニマップにはマトリックスビュー全体が表示されます。ミニマップの薄い灰色の部分は、画面に現在表示されているマトリックスの部分を表します。この領域をドラッグして、マトリックスをスクロールできます。

（注） ミニマップはデフォルトで閉じられています。[Expand] アイコンをクリックして、ミニマップを展開して表示します。

セルを選択すると、[Matrix] ビューによってそのセルと対応する行（送信元スケーラブルグループ）およびカラム（宛先スケーラブルグループ）が強調表示されます。選択したセルの座標（送信元スケーラブルグループおよび宛先スケーラブルグループ）がマトリックスコンテンツ領域の近くに表示されます。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

[Filter] オプションを使用して、選択した一連の送信元および宛先グループのポリシーマトリックスのサブセットを表示できます。フィルタを作成して、関心のあるポリシーだけに絞り込むことができます。フィルタを作成するには、含める送信元および宛先グループを選択します。

Cisco DNA Center と Cisco ISE を統合します。Cisco ISE は、Cisco DNA Center の代わりにネットワークデバイスにポリシーをダウンロードするためのランタイム ポリシー プラットフォームを提供します。ポリシーの同期の問題を防ぐために、セキュリティグループ、セキュリティグループ アクセス コントロール リスト（SGACL）、およびイーグレスポリシーの [TrustSec Workcenter] ユーザーインターフェイス画面が Cisco ISE に読み取り専用モードで表示されます。

ポリシー作成の概要

1. 組織の分類を定義するか、または最初に使用する組織の一部を定義します。
2. 特定した分類のスケーラブルグループを作成します。
3. 制御するネットワークトラフィックのタイプのアクセス契約を作成します。すべてのトラフィックを許可または拒否するためのサンプルアクセス契約が事前に定義されています。また、一部の契約例では、より具体的なトラフィックフィルタリングが示されています。特定のアプリケーション定義に基づいて、さらにきめ細かいアクセス契約を作成できます。
4. アプリケーションサーバーや他のネットワークへの接続など、特定のネットワークリソースへのアクセスを必要とするネットワークユーザーのカテゴリを決定します。
5. アクセスポリシーを作成し、送信元グループ、宛先グループ、およびアクセス契約を関連付け、送信元から宛先へのトラフィックのフローを許可する方法を定義します。

スケーラブルグループの作成

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Group-Based Access Control]** > **[Scalable Groups]** の順に選択します。

ステップ 2 [Create Scalable Group] をクリックします。
[Create Scalable Group] スライドインペインが表示されます。

ステップ 3 [Create Scalable Group] スライドインペインで、スケーラブルグループの名前と説明（オプション）を入力します。

（注） [Name] フィールドでサポートされる文字は次のとおりです：

- 英数字
- アンダースコア (_)

スケーラブルグループ名は英字で開始する必要があります。

Cisco DNA Center タグ値を生成します。必要に応じて、この値を更新できます。指定した値が既存のスケーラブルグループによってすでに使用されている場合は、エラーメッセージが表示されます。有効な範囲は 2 ～ 65519 です。

ステップ 4 このスケーラブルグループに関連付ける**仮想ネットワーク**をドロップダウンリストから選択します。デフォルトでは、デフォルトの仮想ネットワーク（`DEFAULT_VN`）が選択されています。

ステップ 5 スケーラブルグループを Cisco Application Centric Infrastructure（ACI）に伝播する場合は、[Propagate to ACI] チェックボックスをオンにします。

ステップ 6 **[Save]** をクリックします。

[Scalable Groups] ウィンドウには、スケーラブルグループ名、タグ値、割り当てられた仮想ネットワーク、および関連付けられたポリシーが表示されます。このウィンドウでは、スケーラブルグループのサンプルを表示することもできます。それらのスケーラブルグループを使用または削除できます。

スケーラブルグループは、[Scalable Groups] ウィンドウから編集または削除できます。スケーラブルグループの詳細を表示するには、[Scalable Group Name] のリンクをクリックします。スケーラブルグループの詳細を更新するには、[View Scalable Group] ウィンドウで [Edit] をクリックします。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ネットワークデバイスへの変更に関する通知を送信するように要求します。

スケーラブルグループの [Policies] 列のリンクをクリックすると、そのスケーラブルグループとそれが属するポリシーを使用するアクセス制御ルールが表示されます。スケーラブルグループが任意のアクセスポリシーで使用されている場合は、それを削除することはできません。

Cisco ISE との同期が完了していない場合は、スケーラブルグループの横にオレンジ色の三角形のアイコンが表示されます。

Cisco ISE は、 内部エンドポイントグループ（IEPG）を同期し、Cisco ISE に関連付けられている読み取り専用スケーラブルグループを作成することで、ACI から TrustSec ドメインへのパケットをサポートします。これらのスケーラブルグループは、[Created In] 列の値が `ACI` である [Scalable Groups] ウィンドウに表示されます。ACI から学習したスケーラブルグループを編集または削除することはできませんが、ポリシーで使用することはできます。

[Associated Contracts] 列には、ACI から学習したスケーラブルグループに関連付けられている ACI 学習契約が表示されます。[Associated Contracts] 列に表示されるリンクをクリックすると、関連付けられた契約に関する詳細が表示されます。

IEPG が ACI で更新されると、対応するスケーラブルグループ設定が Cisco ISE で更新されます。Cisco ISE でスケーラブルグループが作成されると、新しい EEPG が ACI に作成されます。

（注） 名前が「ANY」またはタグ値が 0xFFFF/65535 のスケーラブルグループを作成することはできません。スケーラブルグループ ANY/65535 は、Cisco DNA Center デフォルトポリシーに使用される予約済みの内部スケーラブルグループです。

Cisco DNA Center でスケーラブルグループを Cisco ISE と同期する場合、次のようになります。

- スケーラブルグループが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- スケーラブルグループが Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco DNA Center と Cisco ISE の両方でスケーラブルグループ名が同じだが、説明と ACI データが異なっている場合は、 Cisco DNA Center が Cisco ISE で指定されたデータを使用して更新されます。
- Cisco DNA Center と Cisco ISE でスケーラブルグループ名が同じだが、タグ値が異なる場合は、Cisco ISE で指定されたタグ値を持つ新しいスケーラブルグループが Cisco DNA Center に作成されます。Cisco DNA Center にすでにあるスケーラブルグループの名前は、サフィックス `_DNAC` で更新されます。
- タグ値が同じだが、スケーラブルグループ名が異なる場合は、Cisco DNA Center のスケーラブルグループ名が Cisco ISE で指定された名前で更新されます。

アクセス契約の作成

アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。Access contracts define the actions（permit or deny）performed when the traffic matches a network application, protocol, and port.

（注） Cisco ISE のセキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco DNA Center のアクセス契約と呼ばれます。

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Create Access Contract] をクリックします。

ステップ 3 [Create Access Contract] スライドインペインで、契約の名前と説明を入力します。

ステップ 4 トラフィックフィルタルールを作成します。

- [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
- From the **APplication** drop-down list, choose the application for which you want to apply that action. ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

  トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1 つの契約に複数のルールを作成するには、[+] 記号をクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルアイコンを使用してドラッグして、ルールの順序を変更します。

[Logging] トグルを使用して、任意のトラフィックフィルタルール（デフォルトアクションを含む）のロギングを有効化または無効化できます。ロギングはデフォルトではディセーブルになっています。ロギングが有効になっている場合、トラフィックフィルタルールにヒットすると、ネットワークデバイスは syslog メッセージを送信します。これは、ポリシーのトラブルシューティングと初期化テストに役立つ場合があります。ただし、ネットワークデバイスのリソースとパフォーマンスに影響を与える可能性があるため、このオプションは慎重に使用することを推奨します。

ステップ 5 [Default Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

必要に応じて、デフォルトアクションのロギングを有効にできます。

ステップ 6 **[Save]** をクリックします。

[Access Contracts] リストウィンドウで、契約の表示、作成、複製、更新、および削除ができます。

また、[Access Contracts] ウィンドウでサンプル契約を表示することもできます。それらのサンプル契約は使用または削除できます。ただし、デフォルトの契約（Permit IP、Deny IP、Permit_IP_Log、Deny_IP_Log）は削除できません。

[Access Contracts] ウィンドウの [Contract Name] リンクをクリックして、契約の詳細を表示します。契約の詳細を編集するには、[View Contract] ウィンドウで [Edit] をクリックします。

Cisco ISE との同期が完了していない場合、契約の横にオレンジ色の三角形のアイコンが表示されます。

ACI から学習した契約は [Access Contracts] ウィンドウに表示され、[Created In] 列の値が [ACI] になります。ACI から学習した契約を編集したり削除したりすることはできませんが、ACI から学習したスケーラブルグループの使用中にポリシーで使用することはできます。マトリックスビューからポリシーを作成または更新する場合に、ACI から学習したスケーラブルグループを接続先グループとして選択すると、関連する契約が [Preferred Contracts] タブに表示されます。[All Contracts] タブですべての契約を確認できます。

[Rules Count] 列で、各契約で使用されているルールの数を確認できます。

契約を使用するポリシーを表示するには、契約の [Policies] 列のリンクをクリックします。

ポリシーで使用されている場合、契約を削除することはできません。契約を削除する前に、そのポリシーから契約を削除する必要があります。

スケーラブルグループ、契約、またはポリシーを更新する場合は、ネットワークデバイスに変更を展開する必要があります。ポリシーを更新し、更新したポリシーを展開しない場合、ポリシーの変更に関する通知はネットワークデバイスに送信されず、ネットワークで現在アクティブになっているポリシーは、Cisco DNA Center に表示されるポリシー情報と一致しない可能性があります。この状況を解決するには、ネットワークデバイスに、更新したポリシーを展開する必要があります。

既存の契約を複製し、必要な詳細を編集して新しい契約を作成することができます。契約を複製すると、既存の契約に含まれるすべての情報がコピーされ、コピーした契約は、既存の契約名の末尾に文字列 `Copy` が付加された名前になります。

[Filter] オプションを使用して、探している契約を検索できます。

Cisco DNA Center のアクセス契約を Cisco ISE と同期している間：

- 契約が Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- コントラクトがに存在Cisco ISEし、にCisco DNA Center存在しない場合は、にCisco DNA Center作成されます。
- 契約名が Cisco DNA Center と Cisco ISE で同じであるが、説明とトラフィックルールの内容が異なっている場合、Cisco DNA Center は Cisco ISE で指定されたデータを使用して更新されます。
- 契約名とルールが同じで、説明が異なっている場合、Cisco DNA Center は Cisco ISE で指定された説明を使用して更新されます。
- Cisco ISE の Text SGACL コマンドラインは、解析できないコンテンツとして移行されます。これらの契約は編集できますが、Cisco DNA Center では構文解析や構文チェックは行われません。Cisco DNA Center で加えた変更は、Cisco ISE に反映されます。

- Cisco ISE でポリシーに複数の SGACL がある場合、それらの契約は Cisco DNA Center のデフォルトポリシーとして移行されます。

グループベースのアクセス コントロール ポリシーの作成

スケーラブルグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセス コントロール ポリシーを作成する際には、以前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作成したりできます。

特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。

たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザーがアクセスできるネットワークリソースを指定する場合は、1 つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。「財務サーバー」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

グループベースのアクセス コントロール ポリシーは、送信元グループと宛先グループの特定ペアのトラフィックフローに基づいて作成または更新することもできます。

グループベースのアクセス コントロール ポリシーを作成するには、次の手順を使用します。

ステップ 1 [Policy List] または [Matrix]ビューで、[Create Policies] をクリックします。

ステップ 2 1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成するには、[Source To Destination(s)] をクリックし、次の手順を実行します。

a) 選択する送信元スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックして、新しいスケーラブルグループを作成します。詳細については、「スケーラブルグループの作成 （7 ページ）」を参照してください。

b) [Next] をクリックします。

c) 選択した送信元スケーラブルグループにマッピングする宛先スケーラブルグループを選択します。

必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。

送信元と宛先の間にポリシーがすでに存在する場合、スケーラブルグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。詳細については、「アクセス契約の作成 （8 ページ）」を参照してください。

必要に応じて、契約の詳細を表示および編集できます。

（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) **[Save]** をクリックします。

ステップ 3 1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成するには、[Destination to Source(s)] をクリックし、次の手順を実行します。

a) 選択する宛先スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックします。

b) **[次へ (Next)]** をクリックします。

c) 選択した宛先スケーラブルグループにマッピングする送信元スケーラブルグループを選択します。

必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。

送信元と宛先の間にポリシーがすでに存在する場合、スケーラブルグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、[Create Contract] をクリックします。

必要に応じて、契約の詳細を表示および編集できます。

（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) **[Save]** をクリックします。

（注） [Scalable Group] リストエリアの右上隅にある [Toggle]ボタンを使用して、[List]ビューと [Drag and Drop]ビューを切り替えることができます。[Drag and Drop] ビューを使用すると、アクセス コントロール ポリシーの作成時に、スケーラブルグループを [Source] フィールドと [Destination] フィールドにドラッグアンドドロップすることができます。ただし、[Drag and Drop]ビューには、最初の 50 のスケーラブルグループのみが表示されます。スケーラブルグループの数が少ない場合（最大 50）は、[Drag and Drop] ビューを使用できます。スケーラブルグループが 50 を超える場合は、[List] ビューを使用してすべてのグループを表示します。

トラフィックフローに基づいてグループベースのアクセス コントロール ポリシーを作成または変更するには、次の手順を実行します。

1. ポリシーマトリックスビューで、グループベースのアクセス コントロール ポリシーを作成または変更するセルをクリックします。
2. [Policy Details] スライドインペインで、[View Traffic Flows] をクリックします。

   [View Traffic Flows] スライドインペインの左側のペインでは、選択した契約のルールまたはデフォルトのポリシーを確認できます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。
3. [Default Action] ルールの [View Traffic] をクリックして、そのルールに一致するフローのリストを表示します。追加のルールを持つアクセス契約を使用して既存のポリシーを変更する際、任意のルールの [View Traffic] オプションを使用して、そのルールに一致するフローのリストを表示することができます。
4. [Default Action] ルール（明示的に選択されたアクセス契約がない）を使用しているポリシーの場合、アクセス契約を選択するか、そのポリシーで使用される新しいアクセス契約を作成することができます。

   アクセス契約の PERMIT または DENY を使用したポリシーの場合、アクセス契約を選択するか、そのポリシーで使用される新しいアクセス契約を作成することができます。

   カスタムアクセス契約を使用したポリシーの場合、選択したアクセス契約を編集できます。

   新しく作成または編集した契約を保存する際は、次のオプションがあります。

   - 変更を既存の契約に保存します。変更は、その契約を参照するすべてのポリシーに影響します。
   - 変更を新しい契約として保存します。変更は現在のポリシーにのみ適用されます。
   - 変更を新しい契約として保存します。変更はどのポリシーにも適用されません。

Cisco DNA Center でポリシーを Cisco ISE と同期する場合、次のようになります。

- ポリシーが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco ISE でポリシー契約が異なる場合、 Cisco DNA Center は Cisco ISE で指定された契約で更新されます。
- ポリシーモード情報（有効、無効、またはモニター）も Cisco ISE からインポートされます。

Cisco ISE には、単一のポリシーに対して複数の SGACL を許可するオプションがあります（このオプションは Cisco ISE ではデフォルトで有効になっていません）。Cisco DNA Center では、単一のポリシーに対して複数のアクセス契約を使用することはサポートされていません。ポリシーの同期中に、Cisco ISE のポリシーに複数の SGACL がある場合、Cisco DNA Center 管理者には、そのポリシーを変更して契約を選択しないようにするオプションがあります（デフォル

トポリシーを使用する場合）。管理者は、ポリシーの同期が完了した後に、そのポリシーに対して新規または既存のアクセス契約を選択できます。

シスコのグループベースポリシー分析

ここでは、シスコのグループベースポリシー分析について詳しく説明します。

概要

グループベースポリシー分析で提供される情報を使用することで、資産間の通信を可視化してグループベースポリシーを作成したり、新しいアクセスコントロールの導入による影響を評価したり、ポリシーで許可する必要があるプロトコルを正確に特定したりできます。

シスコのグループベースポリシー分析では、ネットワーク上の資産のグループとそれらの通信に関する次のような情報が集約されます。

- 相互に通信しているグループ
- 通信の種類
- 特定の資産が属するグループ

インストール

Cisco DNA Center のライセンスの種類は次のとおりです。

- Cisco DNA Essentials
- Cisco DNA Advantage
- Cisco DNA Premier

Cisco DNA Advantage と Cisco DNA Premier には、グループベースポリシー分析パッケージが含まれています。このパッケージは、次のアーカイブ（.tar.gz ファイル）で構成されています。

- バックエンド
- ユーザー インターフェイス
- サマライザパイプライン
- 集約の定義

シスコのグループベースポリシー分析は Cisco DNA Center の一部ですが、デフォルトではインストールされません。Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します **[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。[Policy Applications] で [Group-Based Policy Analytics] まで下にスクロールします。[Install] をクリックしてアプリケーションをインストールします。

ハードウェアとソフトウェアの互換性

プラットフォーム サポート

シスコのグループベースポリシー分析は、次のハードウェア プラットフォームでサポートされています。

- 44 コアのシングルノードクラスタと 3 ノードクラスタ
- 56 コアのシングルノードクラスタと 3 ノードクラスタ
- 112 コアのシングルノードクラスタと 3 ノードクラスタ

これらのプラットフォームは、ここで説明するパフォーマンスと拡張性の要件を満たしている必要があります。

サポートされているハードウェアの詳細については、「Cisco UCS M4 appliances」または「Cisco UCS M5 appliances」を参照してください。

次の表に、Cisco DNA Center およびシスコのグループベースポリシー分析でサポートされるパフォーマンスメトリックをコアプラットフォームごとに示します。NetFlow メトリックは、シスコのグループベースポリシー分析で導入されています。

表 *1*: パフォーマンスメトリック

メトリック	44 コア、3 ノード	56 コア	112 コア
デバイス（NAD）	5000 スイッチが 1000、ルータが 1000、またはその両方の組み合わせ、AP が 4000	8000 スイッチが 2000、ルータが 2000、またはその両方の組み合わせ、AP が 6000	18,000 スイッチが 5000、ルータが 5000、またはその両方の組み合わせ、AP が 12,000
Clients（エンドポイント）	25,000 ワイヤレスが 20,000、有線が 5,000	40,000 ワイヤレスが 30,000、有線が 10,000	100,000 ワイヤレスが 60,000、有線が 40,000
NetFlow/秒	30,000	48,000	120,000

デバイス サポート

シスコのグループベースポリシー分析を使用するには、NetFlow を有効にする必要があります。次の表に、さまざまなネットワークデバイスで NetFlow を有効にする方法を示します。

表 *2:* デバイス サポート

ネットワーク デバイス（**Network Devices**）	シリーズ	**Cisco DNA Center UI** の **[Network Settings]** の **[Telemetry]** セクションでの **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Cisco DNA Center UI** のテンプレートエディタツールを使用した **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
ルータ	Cisco 1000 シリーズ サービス統合型ルータ（ISR1K）	対応	対応	対応	対応
	Cisco 4000 シリーズ サービス統合型ルータ（ISR4K）	対応	対応	対応	対応
	Cisco 1000v シリーズ クラウド サービス ルータ（CSR 1000v）	対応	対応	対応	対応
	Cisco 1000 シリーズ アグリゲーション サービス ルータ（ASR1K）	対応	対応	対応	対応

ネットワークデバイス（**Network Devices**）	シリーズ	**Cisco DNA Center UI** の **[Network Settings]** の **[Telemetry]** セクションでの **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Cisco DNA Center UI** のテンプレートエディタツールを使用した **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
スイッチ	Cisco Catalyst 9200 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9300 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9400 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9500 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 9600 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 2k シリーズ	非対応	対応	該当なし	対応
	Cisco Catalyst 3560 シリーズ	非対応	対応	該当なし	対応
	Cisco Catalyst 3650 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 3850 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 4k シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 6500 シリーズ スイッチ	非対応	対応	対応	対応
	Cisco Catalyst 6800 シリーズ スイッチ	非対応	対応	対応	対応

ネットワークデバイス（**Network Devices**）	シリーズ	**Cisco DNA Center UI** の **[Network Settings]** の **[Telemetry]** セクションでの **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Cisco DNA Center UI** のテンプレートエディタツールを使用した **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
ワイヤレス コントローラ	Cisco 3504 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 5520 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 8540 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco Catalyst 9800 ベースのコントローラ	対応	対応	対応	対応

Cisco ISE

Cisco ISE 2.4 パッチ 7 以降、Cisco ISE 2.6 パッチ 1 以降、および Cisco ISE 2.7 以降がサポートされています。

Cisco StealthWatch

Cisco Stealthwatch 7.x 以降がサポートされています。

ブラウザのサポート

シスコのグループベースポリシー分析は、次の Web ブラウザを備えた 64 ビットの Windows、Macintosh、および Linux システムと互換性があります。

- Google Chrome：バージョン 73.0 以降
- Mozilla Firefox：バージョン 65.0 以降

シスコのグループベースポリシー分析のホームページのナビゲーション

Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Group-Based Access Control]** > **[Analytics]** の順に選択します。

[View Traffic for] に表示されるスケーラブルグループ、Cisco ISE プロファイル、および Stealthwatch ホストグループの数は、過去 14 日間にトラフィックを開始したエンドポイントが少なくとも 1 つあるグループの数です。

（注） [View Traffic for] に表示される数は、設定されているグループの数ではありません。これらの数には、サーバーとしてのみ機能しているような、すべてのエンドポイントが要求に応答しているだけのグループは含まれません。

図 *1* : グループベースポリシー分析のホームページ

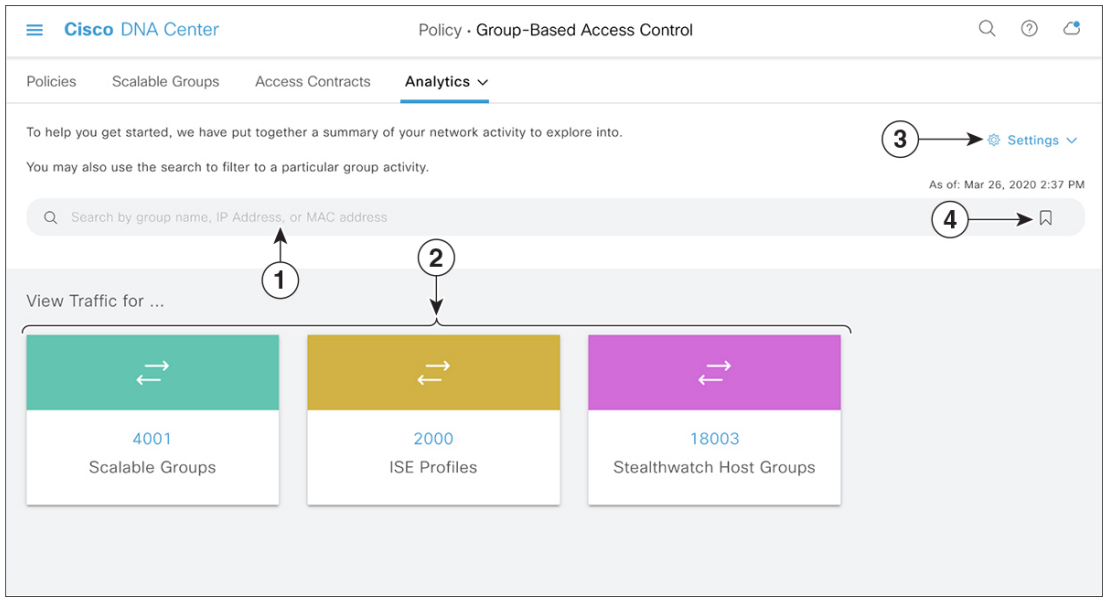
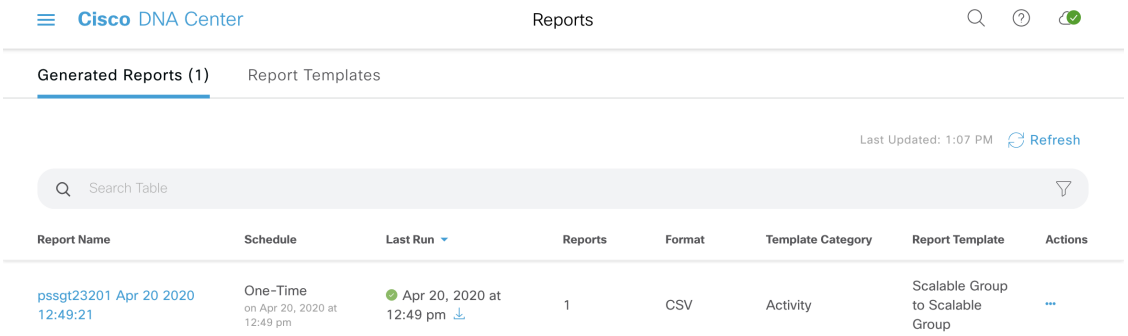


図 1 は、シスコのグループベースポリシー分析のホームページの主な要素を示しています。

1. [Search] フィールドを使用して、さまざまなグループ、IP アドレス、MAC アドレスを検索できます。[Search] フィールドの詳細については、検索の使用をクリックしてください。
2. いずれかのボックスに表示されている数をクリックすると、選択したボックスのグループが送信元でスケーラブルグループを宛先とする複数のグループから複数のグループのウィンドウが表示されます。
3. 次の選択肢があります。

- [Configuration]：このリンクをクリックすると、Cisco ISE、Cisco Stealthwatch、NetFlow などのコレクタを設定または編集できます。
- [Data and Reports]：このリンクをクリックすると、Cisco DNA Center で次の図に示すような [Reports] ウィンドウが開きます。このウィンドウでレポートのステータスを確認できます。また、レポートを編集、複製、実行、ダウンロードすることもできます。



4.  アイコンをクリックすると、保存されているフィルタをロードしたり、現在の検索を保存したりできます。

コネクタについて

シスコのグループベースポリシー分析は、次のソース（コネクタとも呼ばれます）からテレメトリを収集します。コネクタを設定するには、シスコのグループベースのポリシー分析の初期設定 （21 ページ） ワークフローに従うか、**[Policy]** > **[Group-Based Access Control]** > **[Analytics]** > **[Settings]** > **[Configuration]** の順に選択します。

グループデータコネクタ

グループデータコネクタは、資産が分類されるグループに関する情報を収集します。グループデータコネクタには Cisco ISE と Cisco Stealthwatch があります。

- **Cisco ISE**

  Cisco ISE は、アイデンティティおよびアクセス コントロール ポリシーを管理する次世代のプラットフォームとして、企業のコンプライアンス遵守、インフラストラクチャ セキュリティの強化、サービスオペレーションの効率化を実現します。Cisco ISE は、仮想マシンまたは物理マシン、あるいはその両方の組み合わせにインストールされます。Cisco ISE は、Cisco Platform Exchange Grid（pxGrid）サービスを、SessionDirectory、スケーラブルグループ、およびその他の情報を共有するためのパブリッシャ/サブスクライバモジュールとして使用します。PxGrid は、クエリインターフェイスを使用し、一括ダウンロードをサポートしています。ネットワークのユーザーの認証、許可、アカウンティングが行われ、セッションディレクトリが維持されます。ユーザーイベントは、SessionDirectory サービス

に登録されているコネクタにパブリッシュされます。スケーラブルグループ通知などの他のサービスにも登録できます。

ネットワークに入ってきたパケットは、認証で取得したユーザーアイデンティティとデバイスの情報を使用して分類されます。このパケット分類は、パケットがネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータパス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、スケーラブルグループタグ（SGT）と呼ばれることもあります。ネットワークデバイスで SGT に応じてトラフィックをフィルタ処理できるようにすることにより、Cisco ISE でアクセス コントロール ポリシーを適用できるようになります。

さらに、Cisco ISE は、ネットワークに接続されているエンドポイントの情報も収集します。これには、デバイスのタイプ、OS、OS のバージョン、IP アドレスなどの属性が含まれます。これらは ISE プロファイルと呼ばれます。

Cisco ISE コネクタは、シスコのグループベースポリシー分析に使用する SGT の定義とプロファイルを Cisco ISE から提供します。

- **Cisco StealthWatch**

  Cisco Stealthwatch は、高度な脅威検出、脅威への迅速な対応、およびネットワークトラフィックのセキュリティ分析を可能にするネットワークベースの異常検出システムです。Cisco Stealthwatch コネクタは、Cisco Stealthwatch で設定されているホストグループを取得します。ホストグループは基本的に、場所、機能、トポロジなどの類似の属性を持つ複数のホスト IP アドレスまたは IP アドレス範囲の仮想コンテナです。

通信コネクタ

通信コネクタは、グループベースのポリシーの決定に役立つグループ間のトラフィックに関する情報を収集します。これは、Cisco DNA Center で管理しているネットワークデバイスからの NetFlow を使用して実行されます。Cisco DNA Center では、NetFlow がネイティブで収集および集約されます。

シスコのグループベースのポリシー分析の初期設定

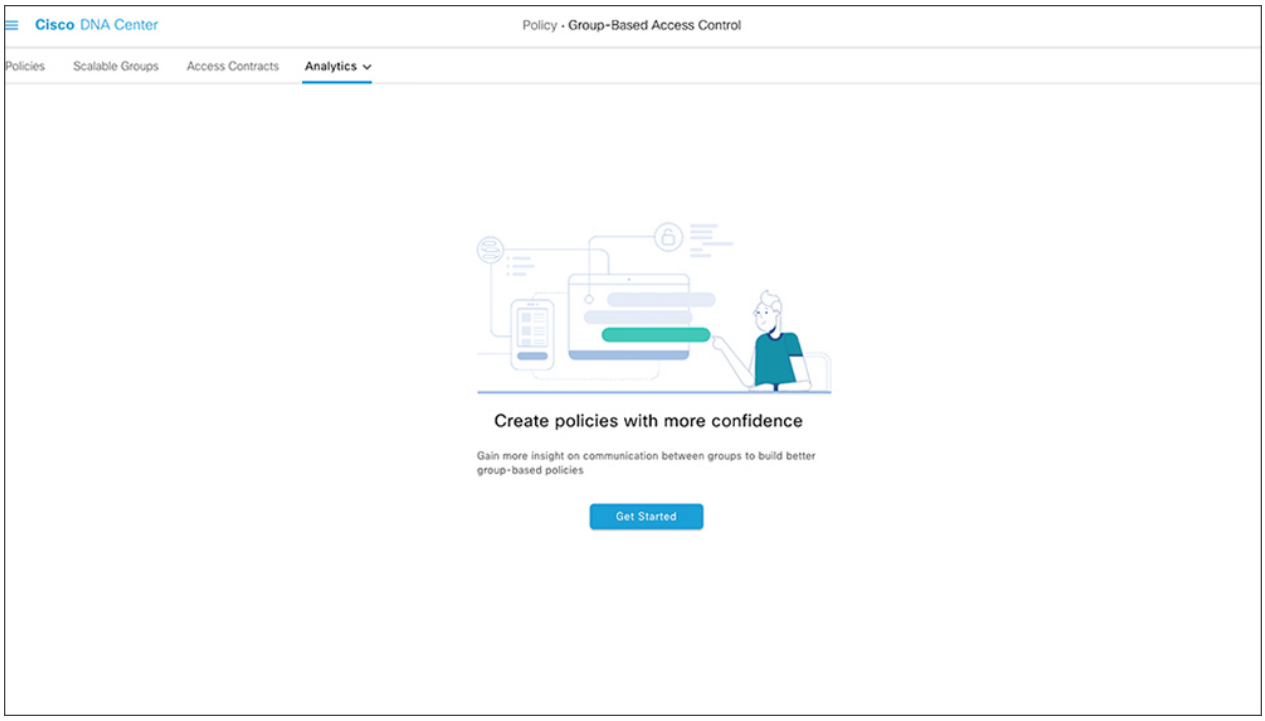
このワークフローでは、Cisco ISE、Cisco Stealthwatch、NetFlow などの特定のソースからネットワークアクティビティやエンドポイントに関連するテレメトリデータを収集するために必要なデータコネクタを設定できます。このタスクは、初めてデータコネクタを設定するときに便利です。

始める前に

Cisco DNA Center にシスコのグループベースポリシー分析がインストールされている必要があります。

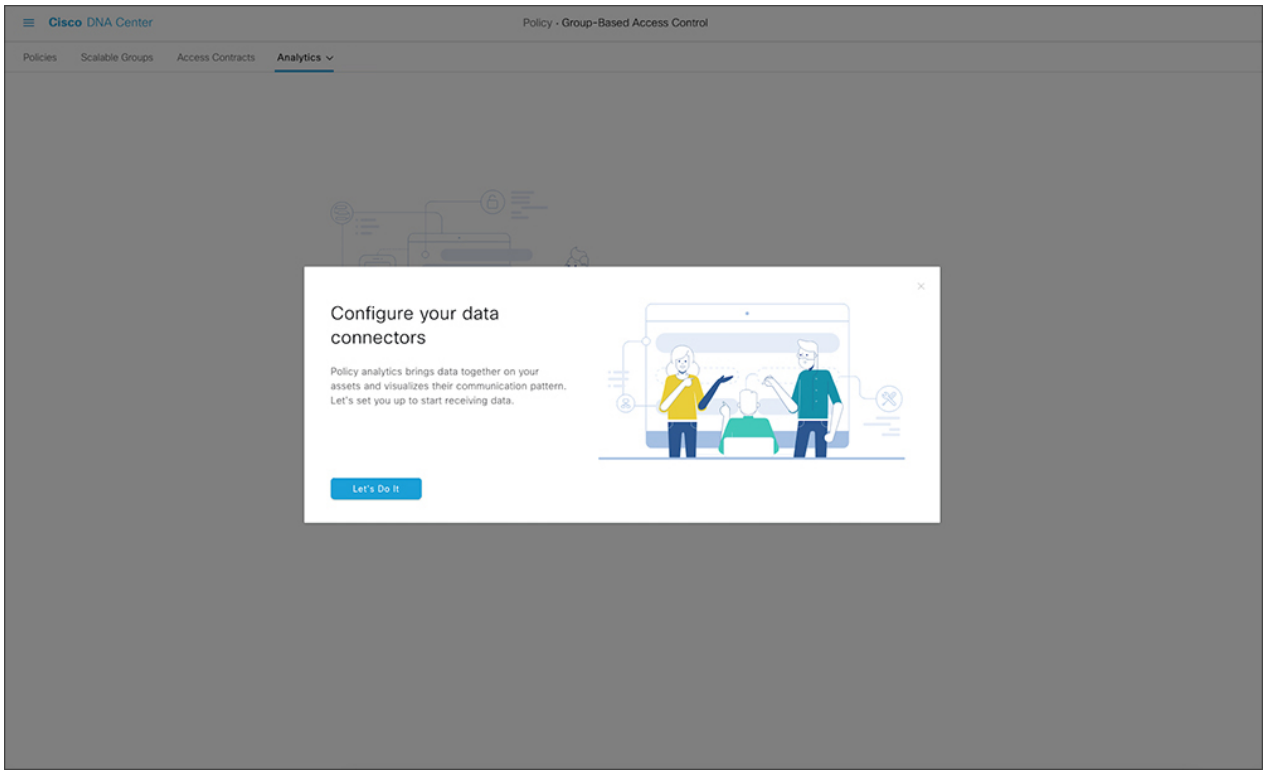
ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Group-Based Access Control]** > **[Analytics]** の順に選択します。[Create policies with more confidence] ウィンドウが表示されます。

図 *2:* 信頼性の高いポリシーの作成



ステップ 2 [Get Started] をクリックします。
[Configure your data connectors] ウィンドウが開きます。

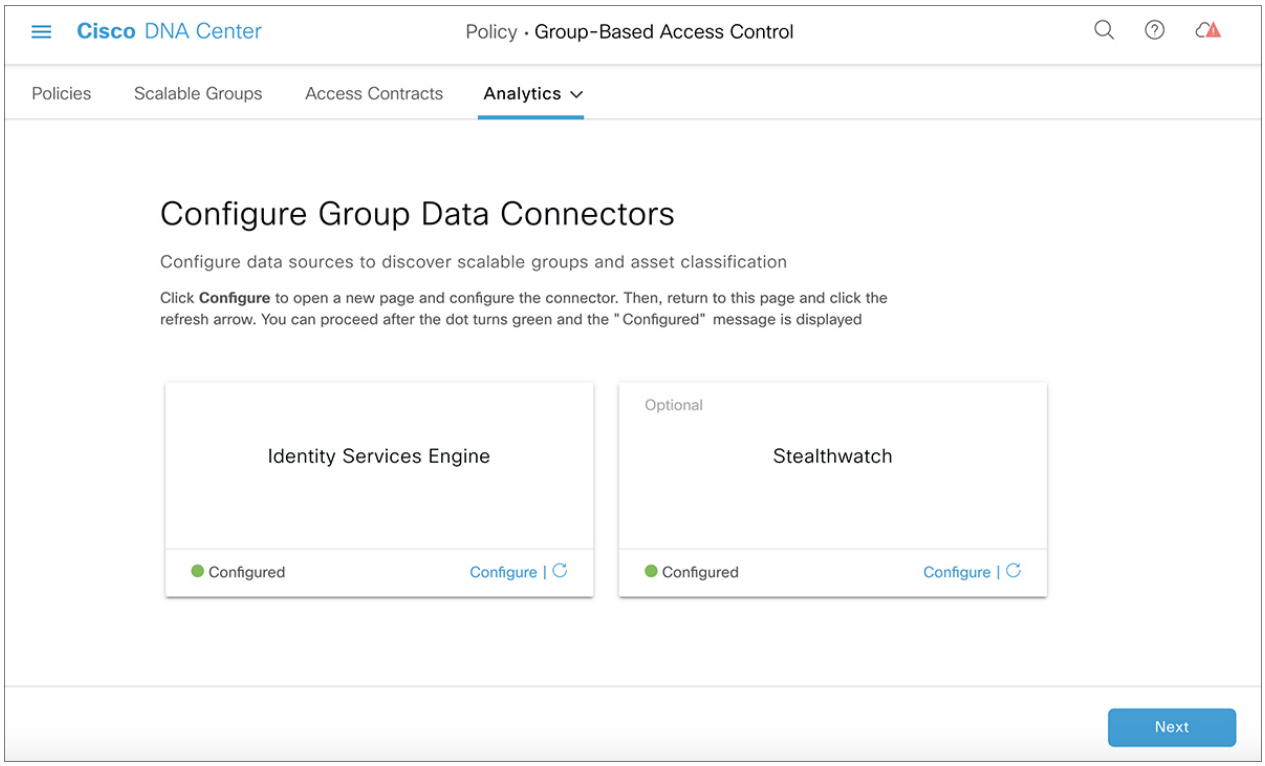
図 *3*: データコネクタの設定



ステップ 3 [Let's Do it] をクリックします。

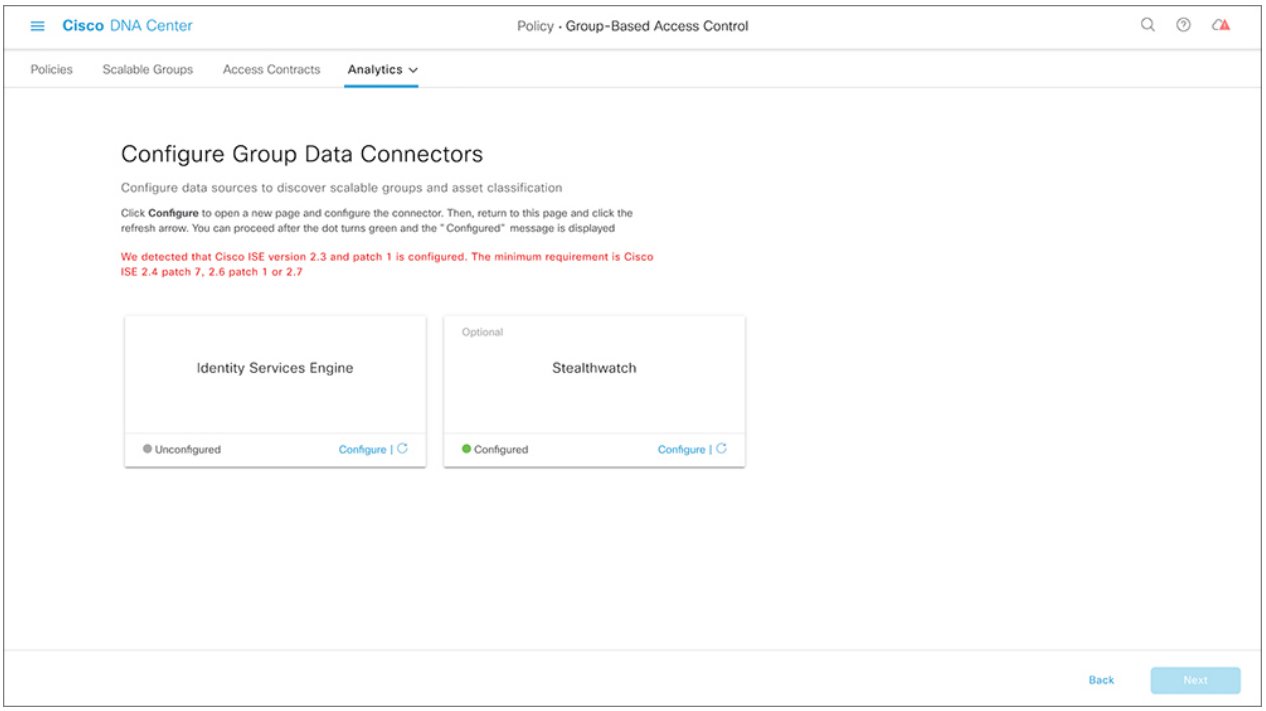
[Configure Group Data Connectors] ウィンドウが開きます。

図 *4:* グループデータコネクタの設定



Cisco DNA Center にインストールされている Cisco ISE のバージョンがシスコのグループベースポリシー分析を実行するために必要なバージョンよりも前のバージョンの場合は、次のエラーが表示されます。

図 *5 : Cisco ISE* のバージョンの要件

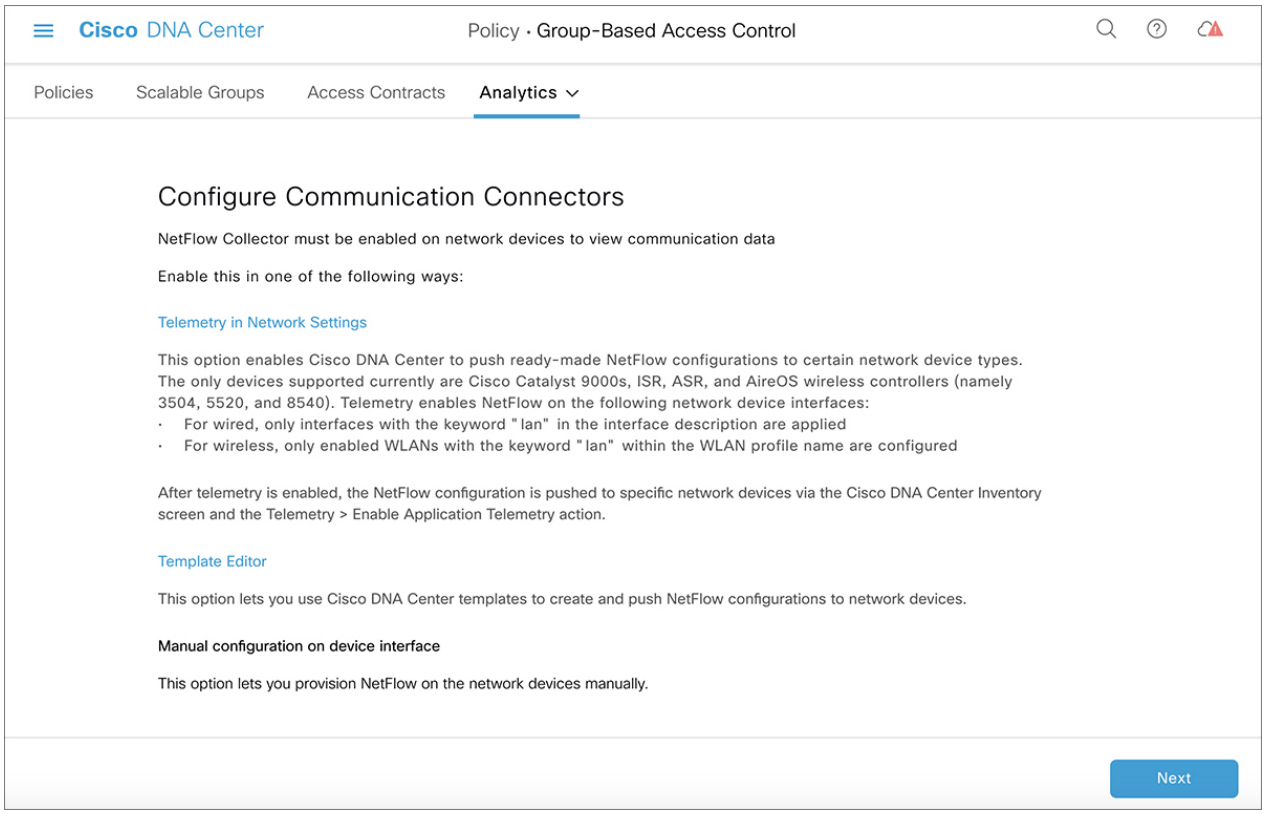


ステップ 4 設定するコネクタの下部にある [Configure] をクリックします。
新しいウィンドウが開き、Cisco DNA Center の [Settings] ウィンドウにリダイレクトされます。ここで必要なコネクタを設定できます。Cisco ISE コネクタを設定する必要があります。Cisco Stealthwatch コネクタの設定は任意です（Cisco ISE コネクタと Cisco Stealthwatch コネクタの両方の設定画面を Cisco DNA Center GUI から利用できます）。

ステップ 5 [Settings] ウィンドウを閉じます。[Configure Group Data connectors] ウィンドウで、正常に設定されたコネクタの [Configure] オプションの横に緑色のドットが表示されます。

ステップ 6 [Next] をクリックします。

図 *6 : Configure Communication Connectors*

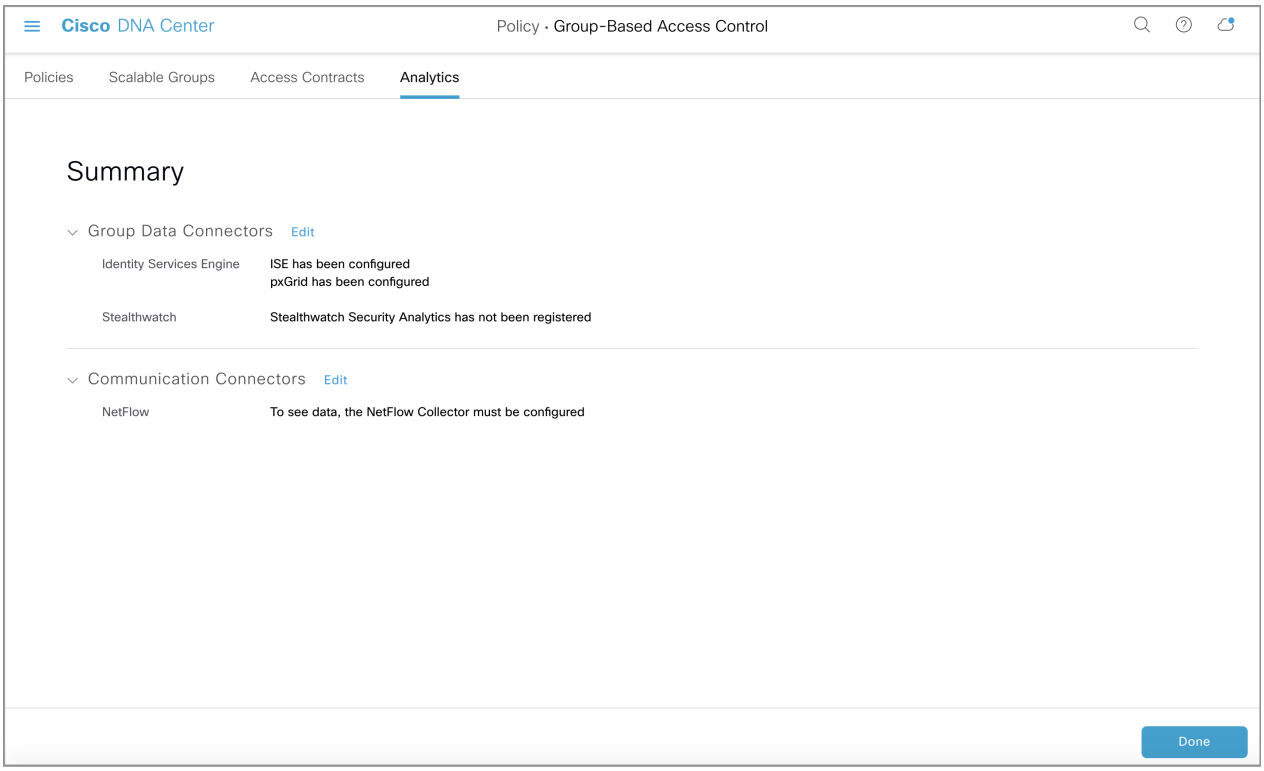


[Configure Communication Connectors] ウィンドウが開きます。

ステップ 7 通信コネクタ（NetFlow）を設定する方法は 3 つあります。Cisco DNA Center のデバイスインターフェイスで手動でプロビジョニングするか、[Template Editor] をクリックして Cisco DNA Center のテンプレートエディタツールで設定するか、[Telemetry in Network Settings] をクリックしてネットワーク設定のテレメトリのセクションで設定します。詳細については、ハードウェアとソフトウェアの互換性（15ページ）の「デバイスサポート」セクションを参照してください。

ステップ 8 [Next] をクリックします。

図 *7 : [Summary]*



コネクタの構成の詳細を示す [Summary] ウィンドウが表示されます。

ステップ 9 グループとエンドポイントの検出を開始するには、[Done] をクリックします。

グループとエンドポイントの確認

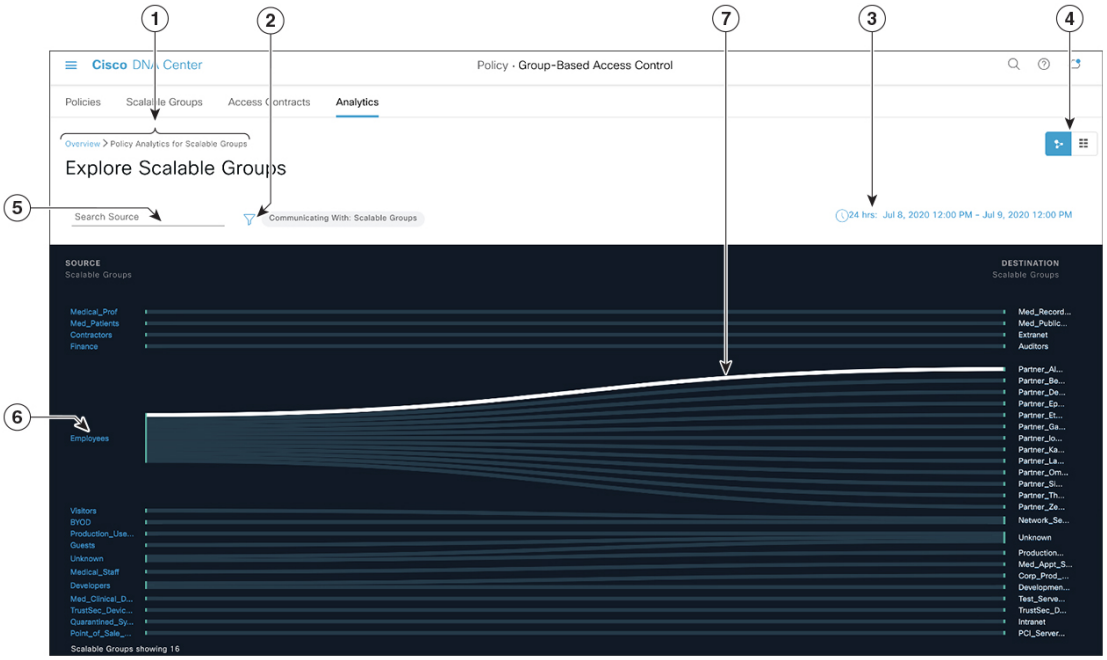
ここでは、各種グループ間のトラフィックを可視化するさまざまな方法について説明します。

複数のグループから複数のグループ

スケーラブルグループからスケーラブルグループ：チャートビュー

ホームページから [Scalable Groups] ボックスに表示されている数をクリックすると、[Explore Scalable Groups] ウィンドウが表示されます。このウィンドウでは、スケーラブルグループについてのすべてのグループ間通信の概要を確認できます。デフォルトでは、過去 24 時間の時間範囲のデータが表示されます。これは、過去 14 日間に設定されたホームページの時間範囲とは異なることに注意してください。チャートには、一意のフローが最も多い送信元スケーラブルグループなどについて、特定の期間における上位 25 の送信元スケーラブルグループとその対応するやり取りが表示されます。次に、このビューの主な要素について説明します。

図 *8*: スケーラブルグループからスケーラブルグループ：チャートビュー

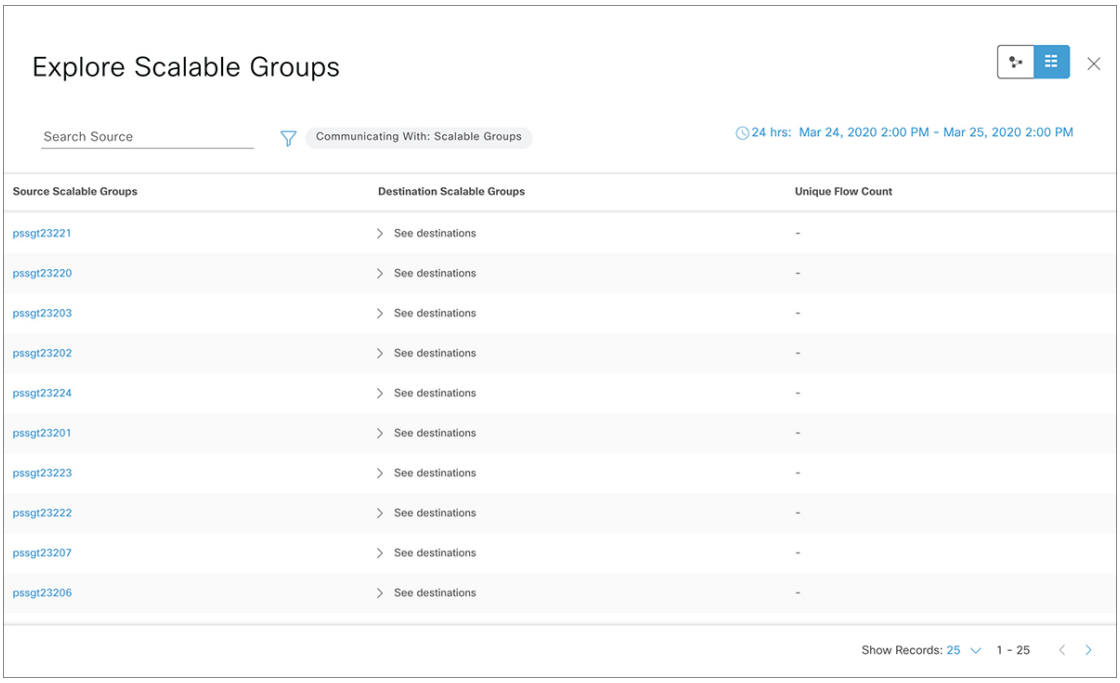


1. トピックパスに従って、シスコのグループベースポリシー分析のホームページのナビゲーションに戻ることができます。
2. アイコンをクリックすると、スケーラブルグループ以外の宛先カテゴリを選択できます。
3. 日時セレクタを使用して日付と時刻を設定できます。
4. アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。
5. ここをクリックして検索語句を入力することで、送信元スケーラブルグループのリストを絞り込むことができます。入力した検索語句がスケーラブルグループに含まれていれば、そのスケーラブルグループが表示されます。
6. 送信元グループをクリックすると、単一のグループから複数のグループのウィンドウが表示されます。
7. リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、単一のグループから単一のグループのウィンドウに切り替わります。

スケーラブルグループからスケーラブルグループ：テーブルビュー

アイコンをクリックすると、次のウィンドウが表示されます。

図 *9 :* スケーラブルグループからスケーラブルグループ：テーブルビュー

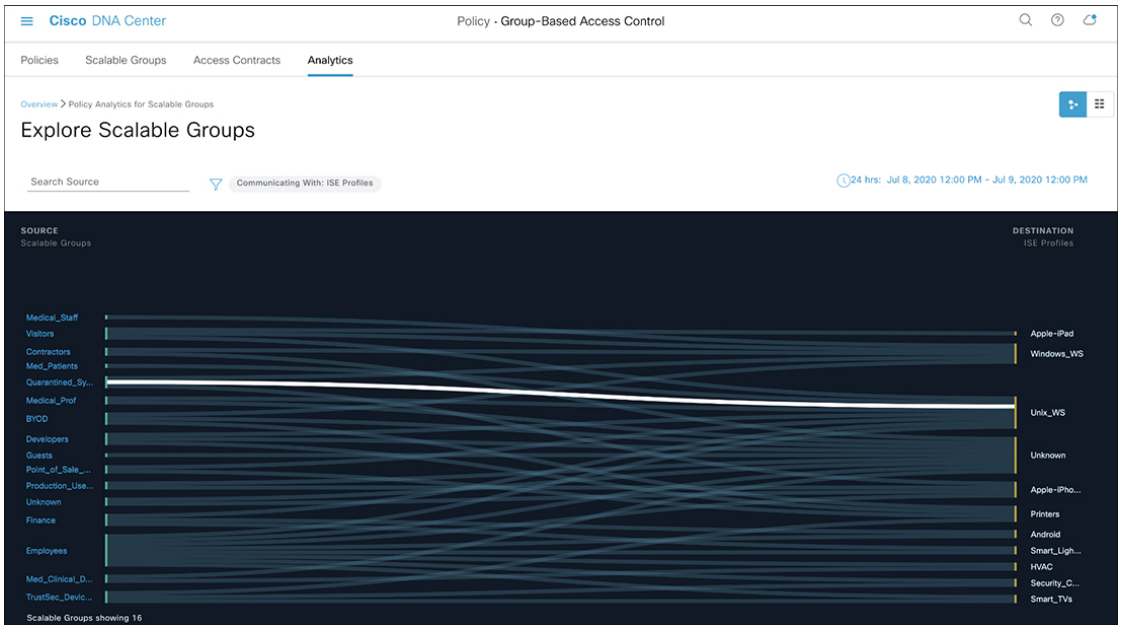


特定の行の [See destinations] リンクをクリックすると、選択した送信元スケーラブルグループに対応するすべての宛先スケーラブルグループが表示されたウィンドウが開き、各宛先スケーラブルグループの一意のフローの数が表示されます。このウィンドウの残りの要素は、チャートビューに表示されるものと同じです。

ISE プロファイルからスケーラブルグループ

ホームページから [ISE Profiles] ボックスに表示されている数をクリックすると、[Explore ISE Profiles] ウィンドウが表示されます。このウィンドウでは、送信元が ISE プロファイルで宛先がスケーラブルグループであるすべての通信の概要を確認できます。

図 *10 : ISE* プロファイルからスケーラブルグループ：チャートビュー

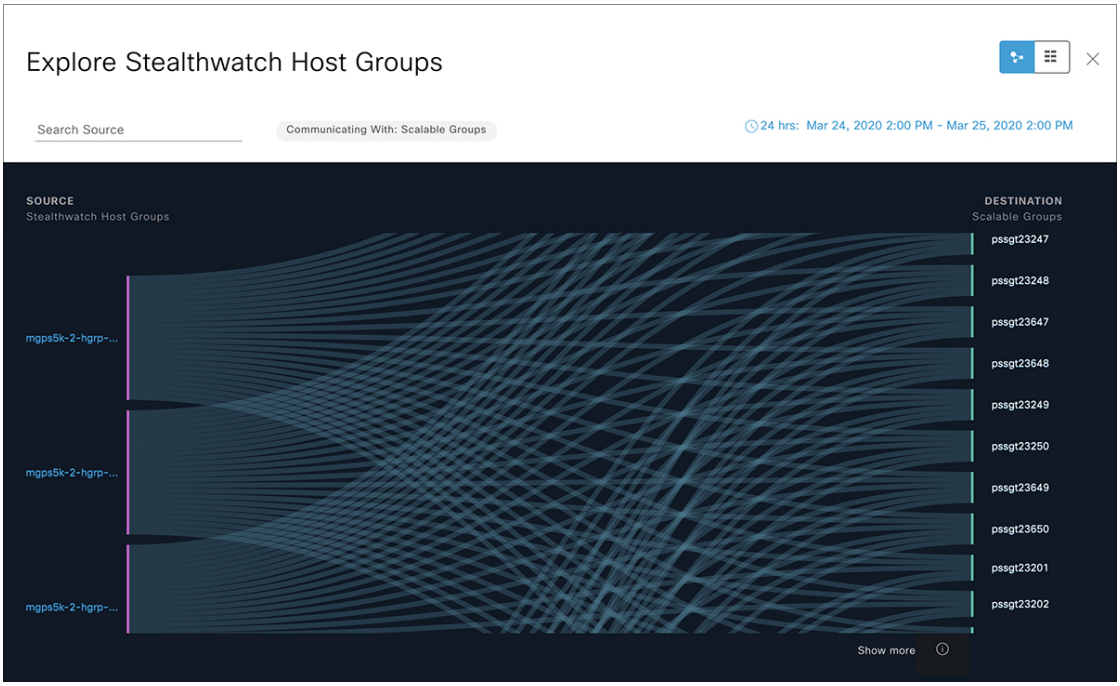


グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをスケーラブルグループにする必要があります。上記のチャートでは、送信元としてISEプロファイルが選択されているため、宛先カテゴリをスケーラブルグループにする必要があります。したがって、このビューには アイコンは必要ありません。

Stealthwatch ホストグループからスケーラブルグループ

ホームページから [Stealthwatch Host Groups] ボックスに表示されている数をクリックすると、[Explore Stealthwatch Host Groups] ウィンドウが表示されます。このウィンドウでは、送信元が Stealthwatch ホストグループで宛先がスケーラブルグループであるすべての通信の概要を確認できます。

図 *11 : Stealthwatch* ホストグループからスケーラブルグループ：チャートビュー



グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをスケーラブルグループにする必要があります。上記のチャートでは、送信元として Stealthwatch ホストグループが選択されているため、宛先カテゴリをスケーラブルグループにする必要があります。したがって、このビューには アイコンは必要ありません。

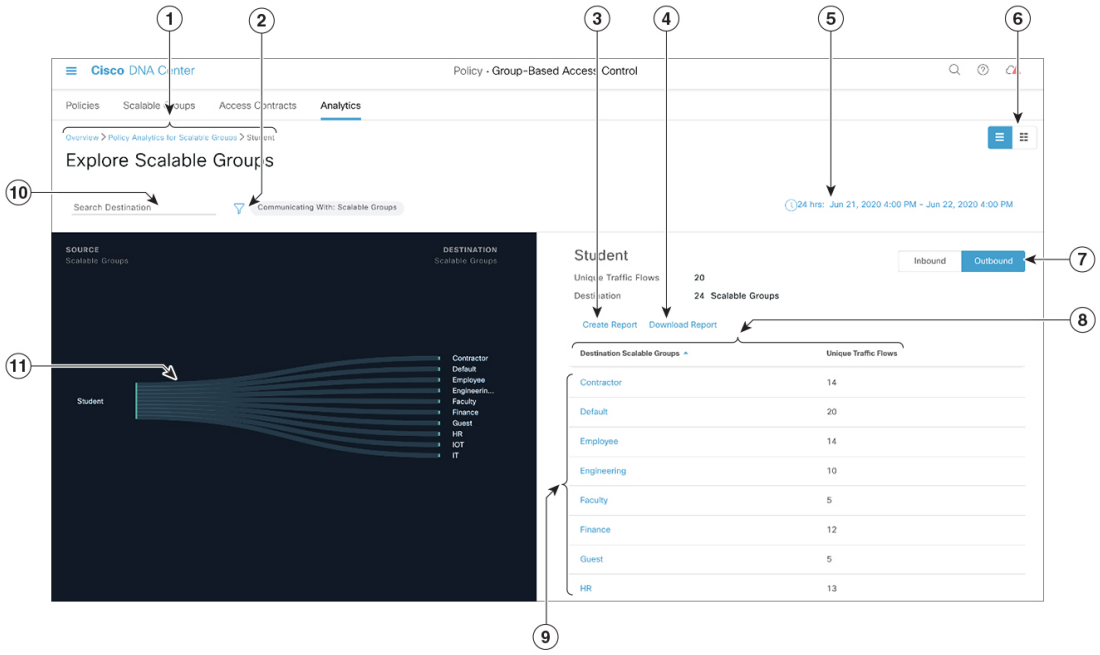
単一のグループから複数のグループ

単一のグループから複数のグループ：アウトバウンド

ここでは、単一の送信元グループと複数の宛先グループの間のアクティビティを確認する際に表示されるウィンドウの要素について説明します。送信元と宛先の少なくとも一方がスケーラブルグループである必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。

次の例は、送信元と宛先の両方が**スケーラブルグループ**の場合の単一のグループから複数のグループのウィンドウを示しています。

図 *12 :* 単一のグループから複数のグループ：アウトバウンド



1. トピックパスに従って、複数のグループから複数のグループに戻ることができます。
2. アイコンをクリックすると、宛先スケーラブルグループ、ISE プロファイル、または Stealthwatch ホストグループを選択できます。
3. [Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。
4. [Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。
5. 日時セレクタを使用して日付と時刻を設定できます。
6. アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。
7. [Outbound] をクリックすると、選択したスケーラブルグループから開始された接続が表示されます。[Inbound] をクリックすると、このスケーラブルグループに対して別のグループから開始された接続が表示されます。
8. 任意の列をクリックして、昇順または降順で並べ替えることができます。
9. グループをクリックすると、選択したグループを宛先とする単一のグループから単一のグループのウィンドウが表示されます。送信元グループは変わりません。

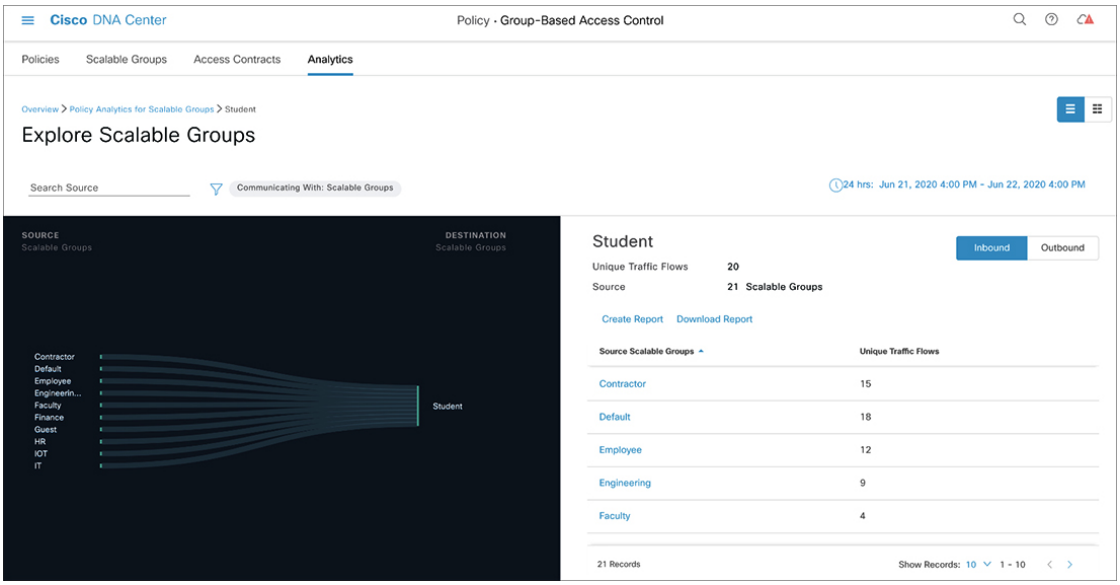
10. ここに検索語句を入力することで、宛先スケーラブルグループのリストを絞り込むことができます。入力した検索語句がこのビューのスケーラブルグループに含まれていれば、そのスケーラブルグループが表示されます。

11. リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、単一のグループから単一のグループのウィンドウに切り替わります。

単一のグループから複数のグループ：インバウンド

[Inbound] をクリックすると、次の図に示すように、選択したスケーラブルグループを宛先としていずれかのグループから開始されたすべての接続が表示されます。

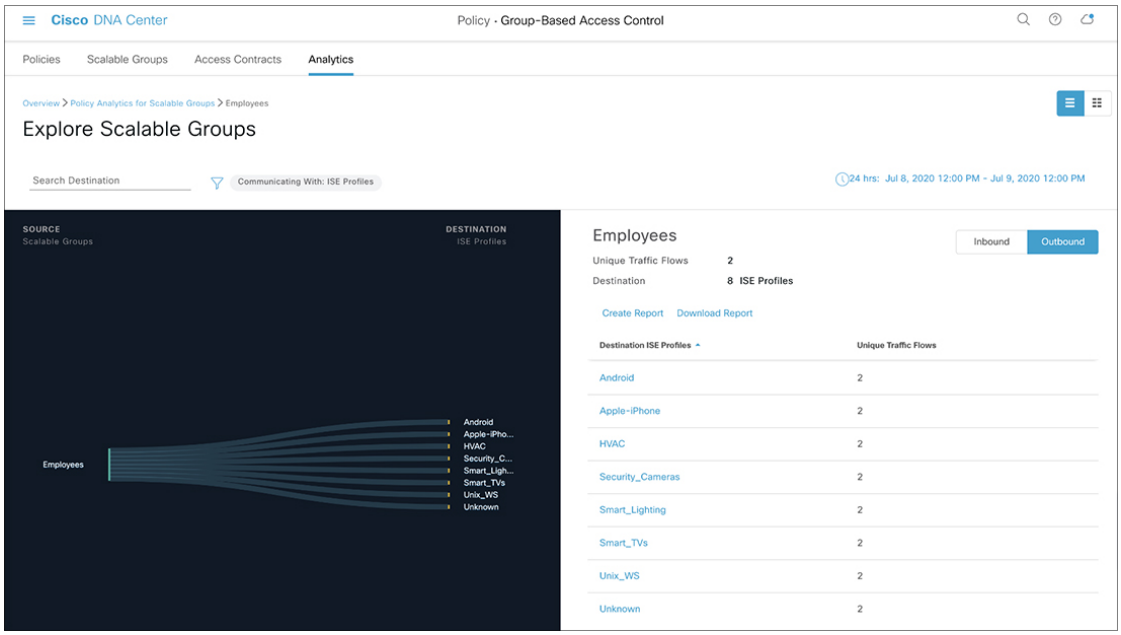
図 *13 :* 単一のグループから複数のグループ：インバウンド



単一の ISE プロファイルから複数のスケーラブルグループ：チャートビュー

アウトバウンド方向の送信元として ISE プロファイルを選択し、宛先としてスケーラブルグループを選択した場合、次のようなウィンドウが表示されます。

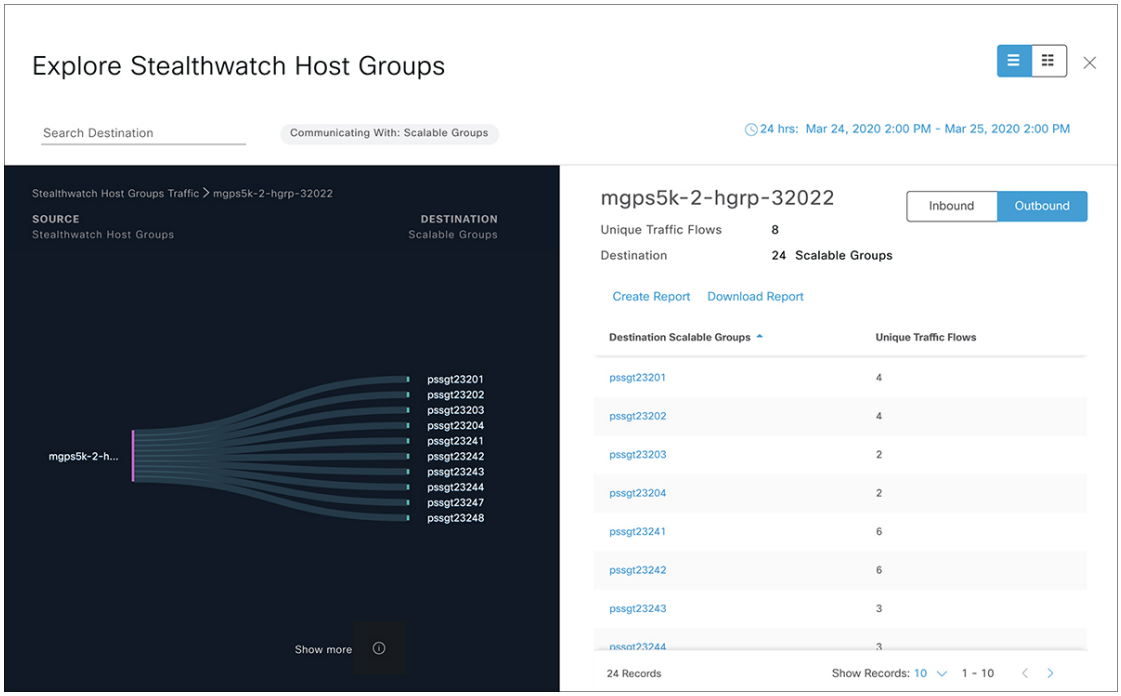
図 *14* : 単一の *ISE* プロファイルから複数のスケーラブルグループ：チャートビュー



単一の Stealthwatch ホストグループから複数のスケーラブルグループ：チャートビュー

アウトバウンド方向の送信元として Stealthwatch ホストグループを選択し、宛先としてスケーラブルグループを選択した場合、次のようなウィンドウが表示されます。

図 *15* : 単一の *Stealthwatch* ホストグループから複数のスケーラブルグループ：チャートビュー



単一のグループから単一のグループ

この [Explore Scalable Groups] ウィンドウには、単一の送信元グループと単一の宛先グループの間のアクティビティが表示されます。送信元グループと宛先グループの少なくとも一方がスケーラブルグループである必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。

リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。

送信元グループと宛先グループの間に表示されている方向矢印をクリックすると、このビューの送信元グループと宛先グループが入れ替わります。

[Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。

[Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。

[View Contract] をクリックして、[View Contract] ウィンドウを起動します。[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。右側のペインでは、ポートとプロトコルの詳細も確認できます。契約の詳細については、「アクセス契約」を参照してください。

 アイコンをクリックするとチャートビューが表示され、  をクリックするとテーブルビューが表示されます。

日時セレクタを使用して日付と時刻を設定できます。

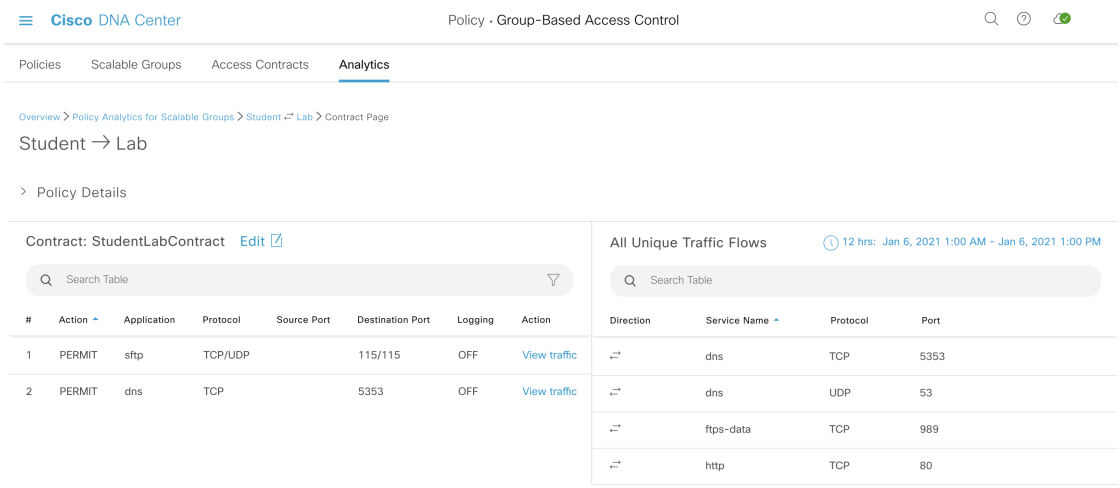
アクセス契約

アクセス契約は [Analytics] タブから直接作成および変更できるようになりました。

View Contract

[View Contract] ウィンドウを起動するには、[Explore Scalable Groups] ウィンドウで [View Contract] をクリックします。[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。

図 *16 : View Contract*



この表には [Policies] ウィンドウからもアクセスできます。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Group-Based Access Control]** > **[Policies]** の順に選択します。

ポリシーマトリックスビューで、契約を作成または変更するセルをクリックします。[Policy Details] スライドインペインで、[View Traffic Flows] をクリックします。

現在、送信元グループと宛先グループの間に契約が割り当てられていない場合、データは表示されません。[Change Contract] または [Create Access Contract] オプションを使用して、契約を作成または変更することができます。

[Action] 列の [View traffic] をクリックして、そのルールに一致するフローのリストを表示します。

アクセス契約の作成

[Contract Content] ウィンドウを起動するには、[Policy Details] ペインで [Create Access Contract] をクリックします。トラフィックフィルタルールを作成するには、次の手順を実行します。

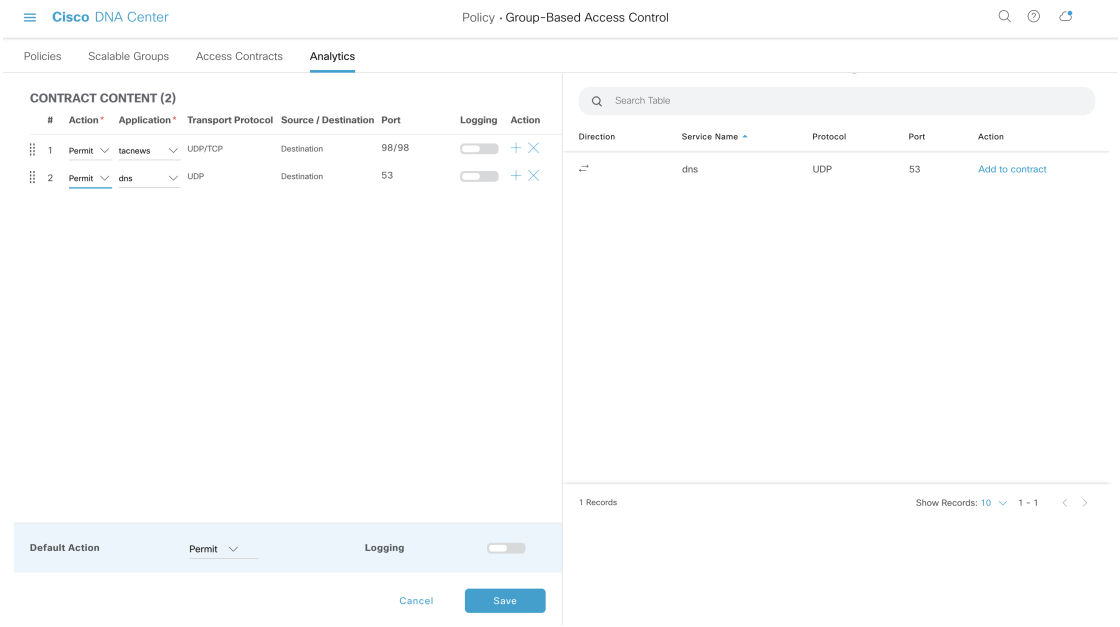
- [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
- From the **APplication** drop-down list, choose the application for which you want to apply that action. ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

  トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1 つの契約に複数のルールを作成するには、プラスのアイコンをクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルのアイコンを使用して、ルールをドラッグして順序を変更します。

[All Unique Traffic Flows] ペインの [Add to Contract] オプションを使用して契約にエントリを追加することができます。

図 *17* : アクセス契約の作成



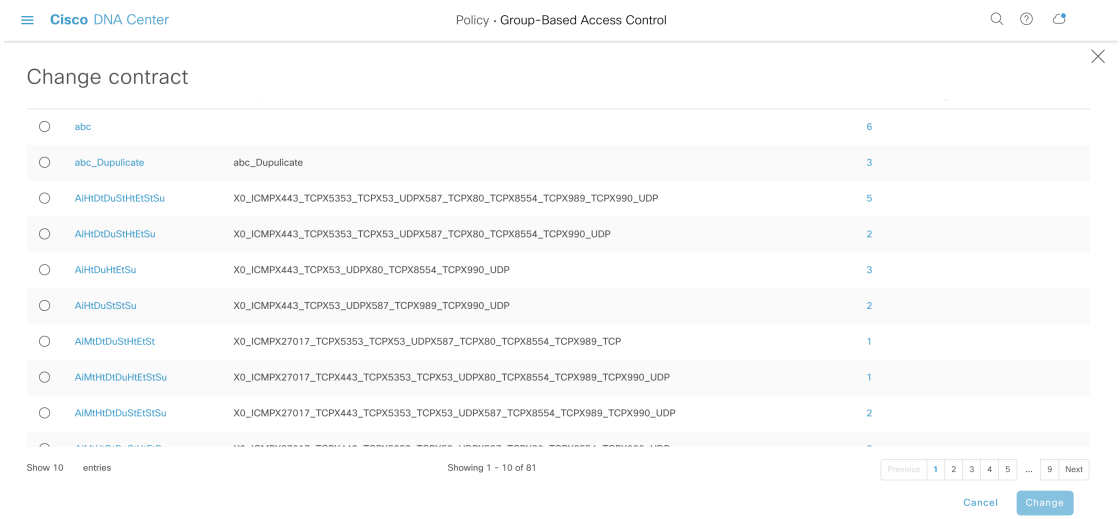
新しく作成または編集した契約を保存する際は、次のオプションがあります。

- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [Update contract for all referenced policies]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

契約の変更

[Change Contract] ウィンドウを起動するには、[Policy Details] ペインで [Change Contract] をクリックします。使用可能なすべての契約が表示されます。必要な契約を選択し、[Change] をクリックすると、その契約をポリシーに追加できます。

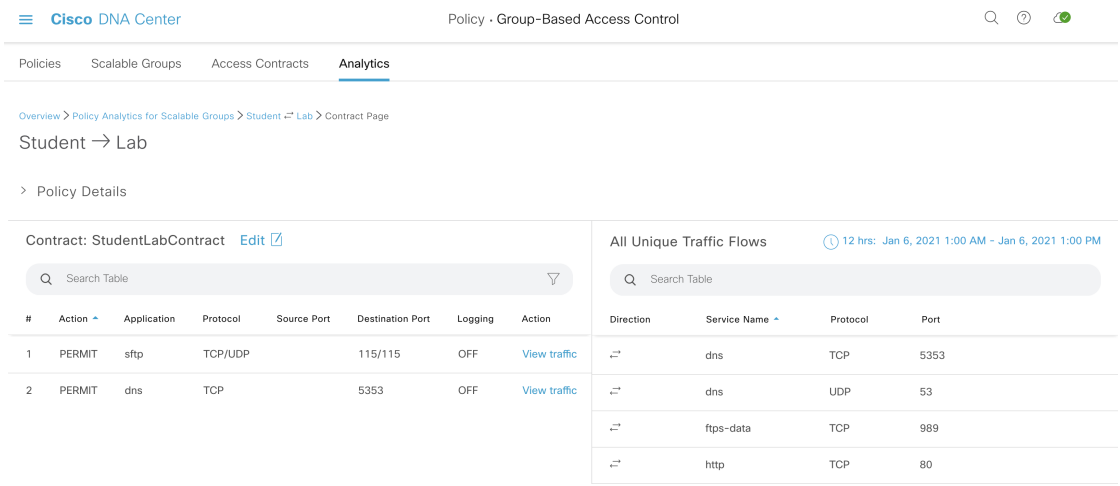
図 *18 :* 契約の変更



契約の編集

[Edit] オプションは、契約がすでにポリシーに追加されている場合にのみ表示されます。契約の詳細を編集するには、契約の名前の後に表示される [Edit] をクリックします。

図 *19 :* 契約の編集



契約を更新したら、[Save] をクリックします。次のオプションを使用できます。

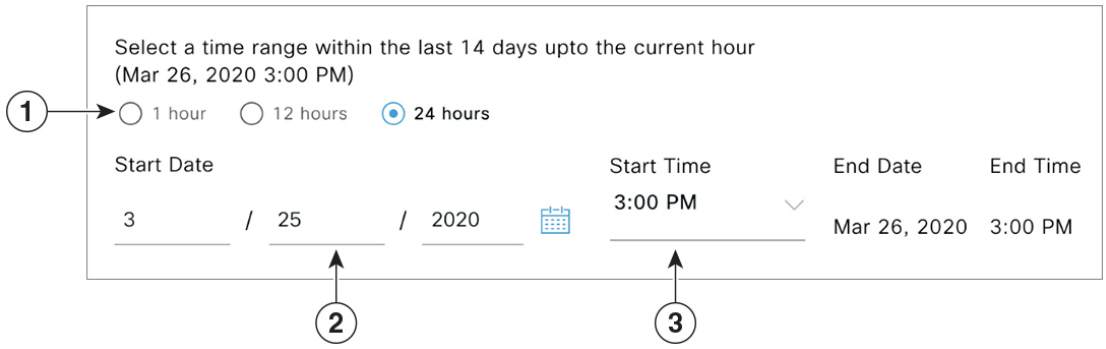
- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [Update contract for all referenced policies]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

適切なオプションを選択した後に、名前と説明を入力し（1 つ目または 3 つ目のオプションを選択した場合）、[Confirm] をクリックします。

日時セレクタ

接続の概要を表示する期間を選択できます。過去 14 日から現在の 1 時間までの時間範囲を選択できます。

図 *20 :* 日時セレクタ

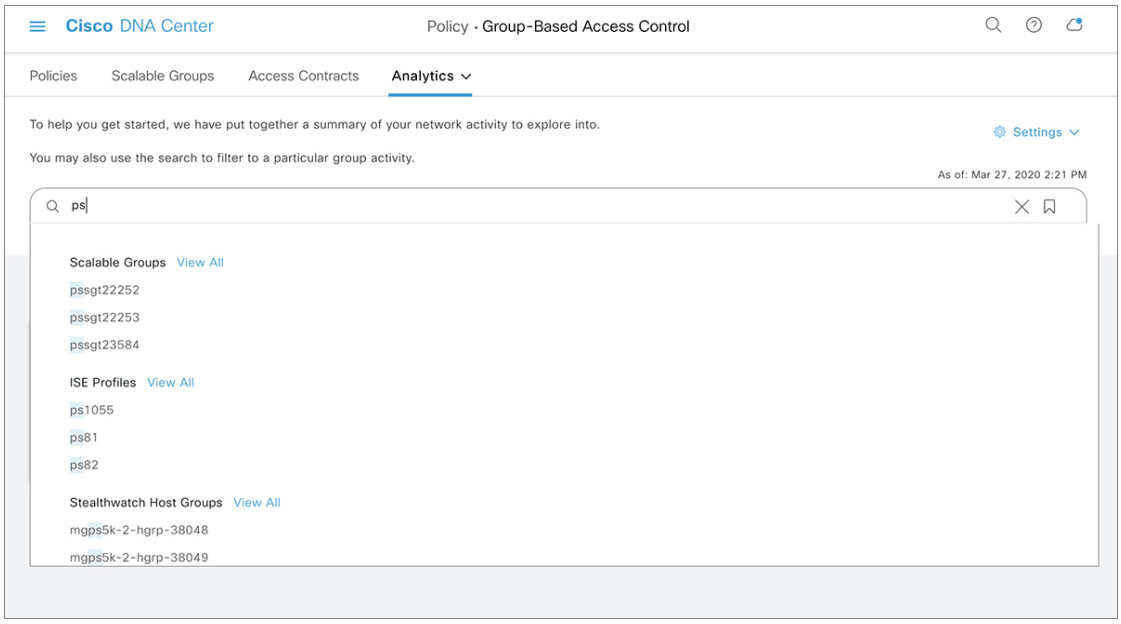


1. 3 つの固定時間範囲のいずれかを選択します。[End Time] は自動的に調整されます。
2. 月、日、年を手動で入力するかカレンダーアイコンを使用して [Start Date] を指定します。
3. [Start Time] をドロップダウンメニューから選択します。

検索の使用

シスコのグループベースポリシー分析のホームページには、スケーラブルグループ、ISE プロファイル、Stealthwatch ホストグループ、IP アドレス、または MAC アドレスのデータ全体を検索するための [Search] フィールドが用意されています。

図 *21* : 検索フィールド



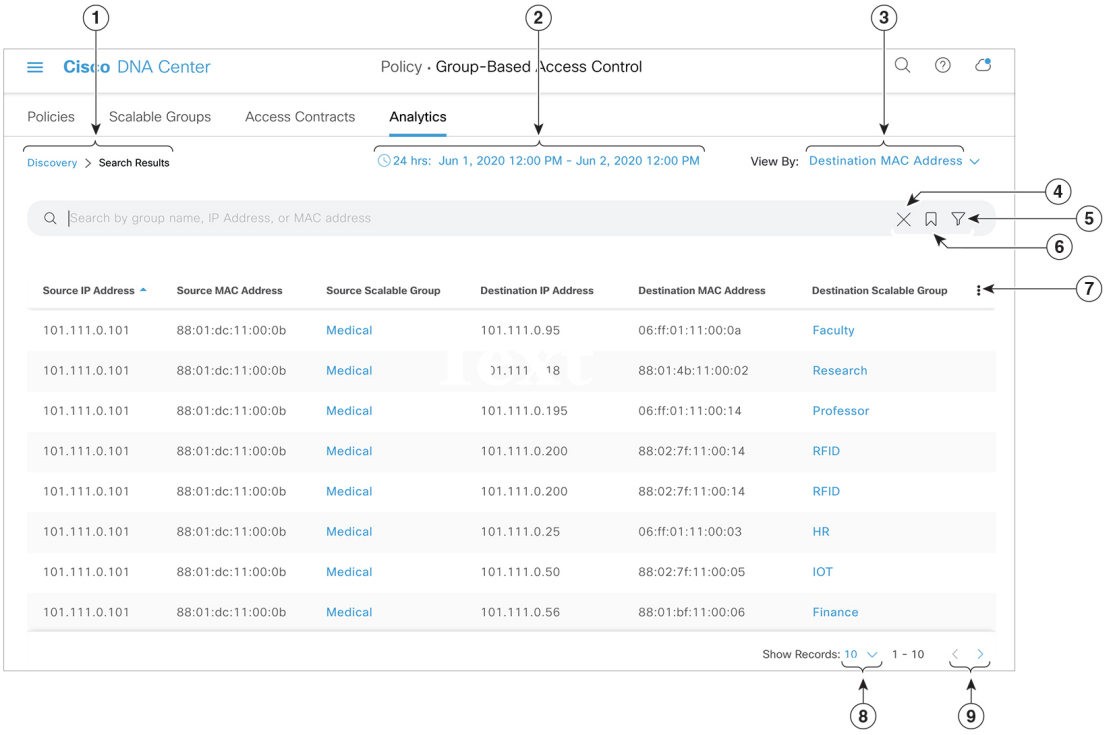
検索フィールドへの文字入力を開始すると、スケーラブルグループ、ISE プロファイル、および Stealthwatch ホストグループの自動検索が実行され、グループタイプごとに最大 3 件の結果が表示されます。検索結果を表示する [View All] リンクは、検索フィールドで関連文字が識別された場合にのみ表示されます。IP アドレスの場合、関連文字は整数とピリオドです。MAC アドレスの場合、関連文字は 16 進数とコロンです。

（注）

- [Search Results] ウィンドウは、[View All] リンクをクリックするまで開きません。
- 読み取り専用ユーザーは、IP アドレスや MAC アドレスは検索できません。詳細については、「ロールベース アクセス コントロール」を参照してください。

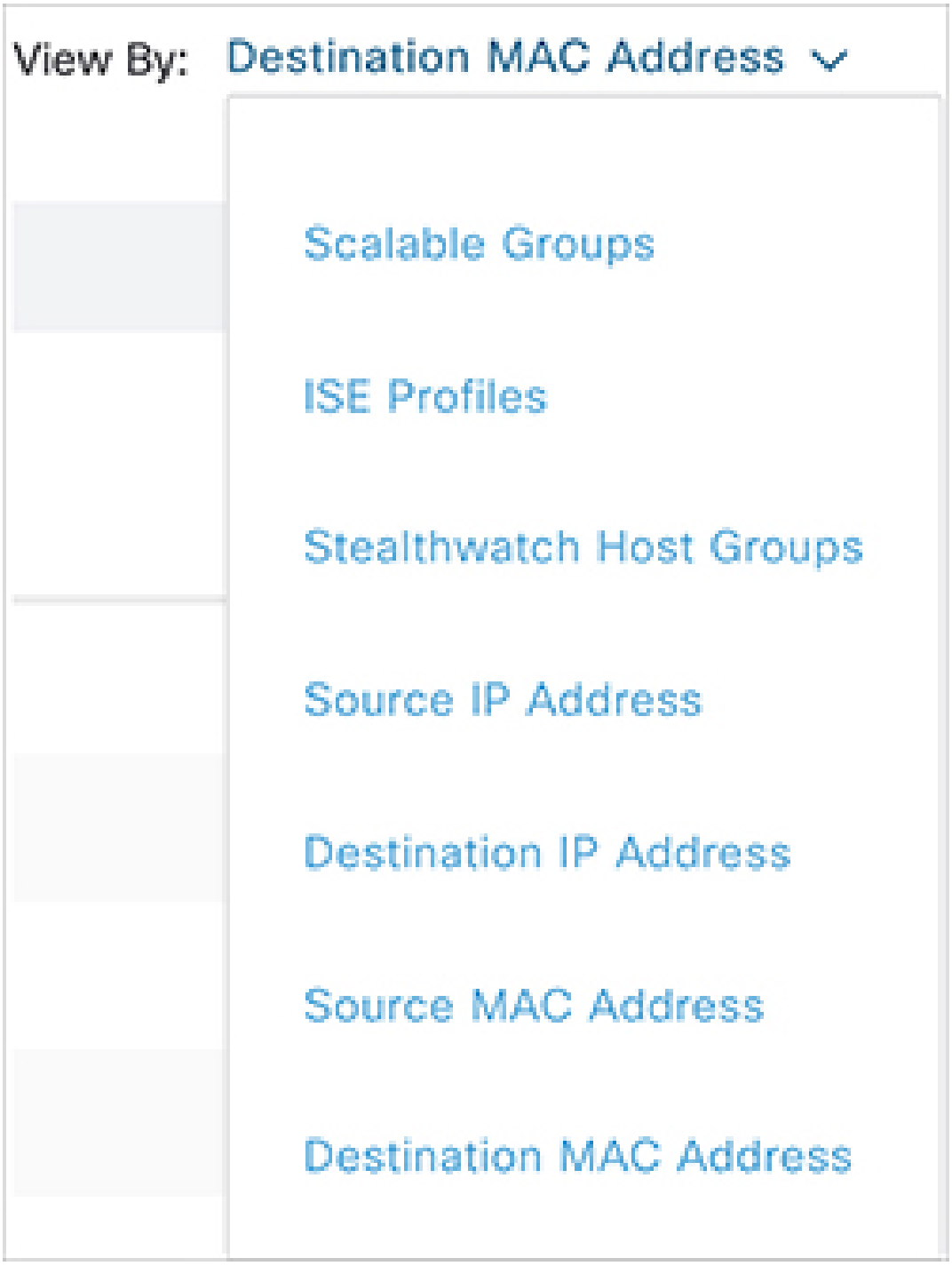
次に、[Search Results] ウィンドウの主な要素について説明します。

図 *22* : 検索結果



1. トピックパスに従って、ホームページに戻ることができます。
2. 日時セレクタを使用して日付と時刻を設定できます。
3. [View By] ドロップダウンリストから、検索条件を変更するために必要なオプションを選択します。選択できるオプションは、次のとおりです。

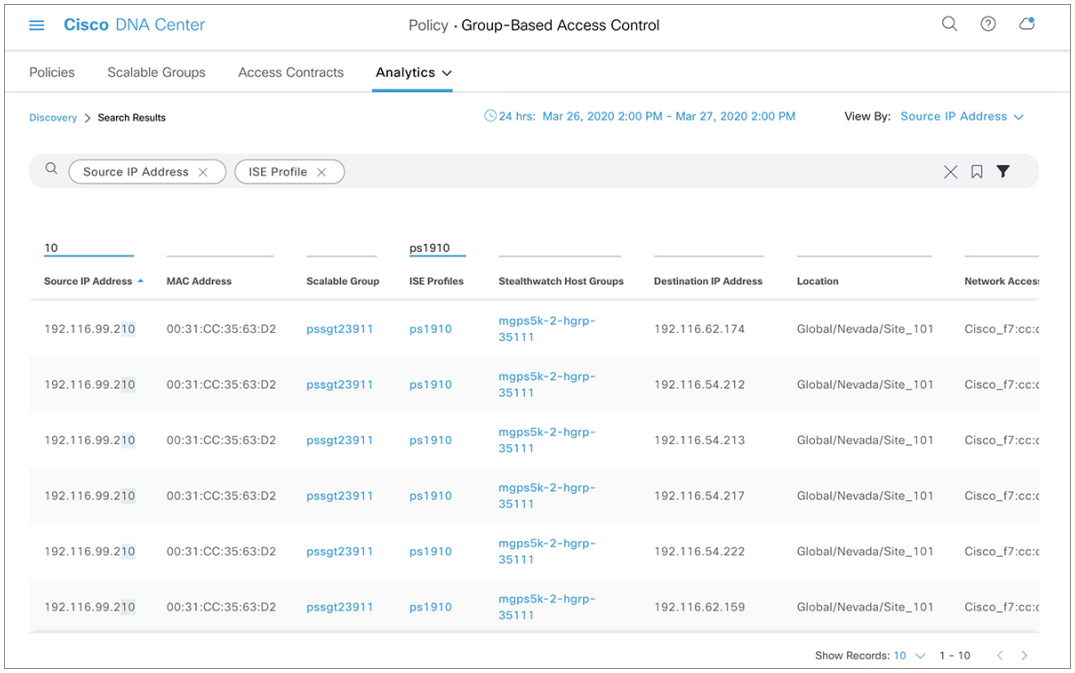
図 *23* : 表示方法



4. 検索結果を閉じるには、 アイコンを使用します。

5. フィルタのアイコン（ ）は高度なフィルタ処理に使用され、MACアドレスまたはIPアドレスを検索する場合にのみ使用できます。 アイコンをクリックすると、各列の列名の上に検索フィールドが表示されます。

図 *24 :* 複数の検索条件

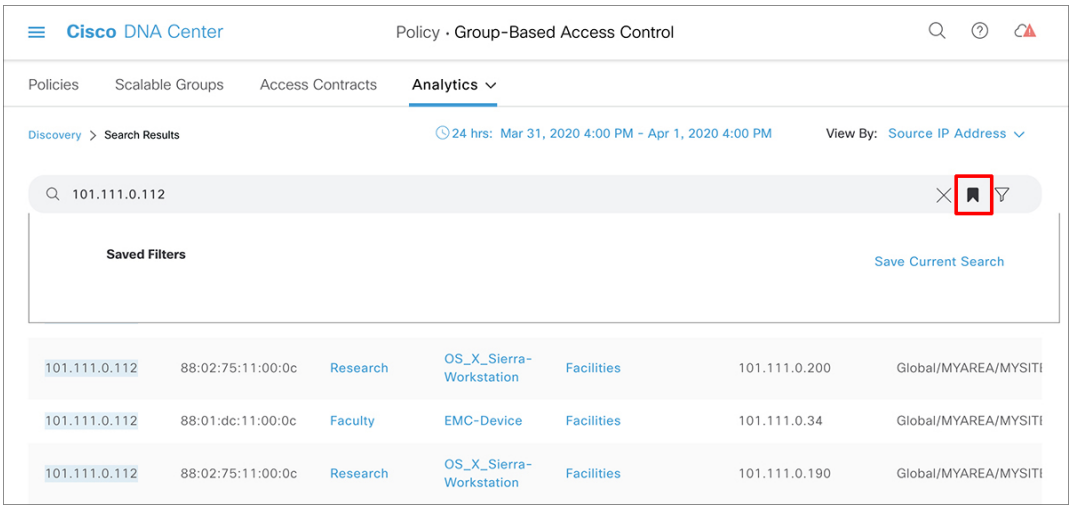


列ごとの検索条件は、最大 3 つまで入力できます。列ごとの条件を複数入力する場合は、OR 演算または AND 演算を指定できます。このように作成したクエリでは、複数の列を対象に AND 演算が実行されます。上図のクエリは、IP アドレスに *10* を含み、ISE プロファイルに *ps1910* を含むエントリと一致します。

6. ブックマーク（ ）アイコンを使用すると、保存されているフィルタをロードしたり、現在の検索を保存したりできます。

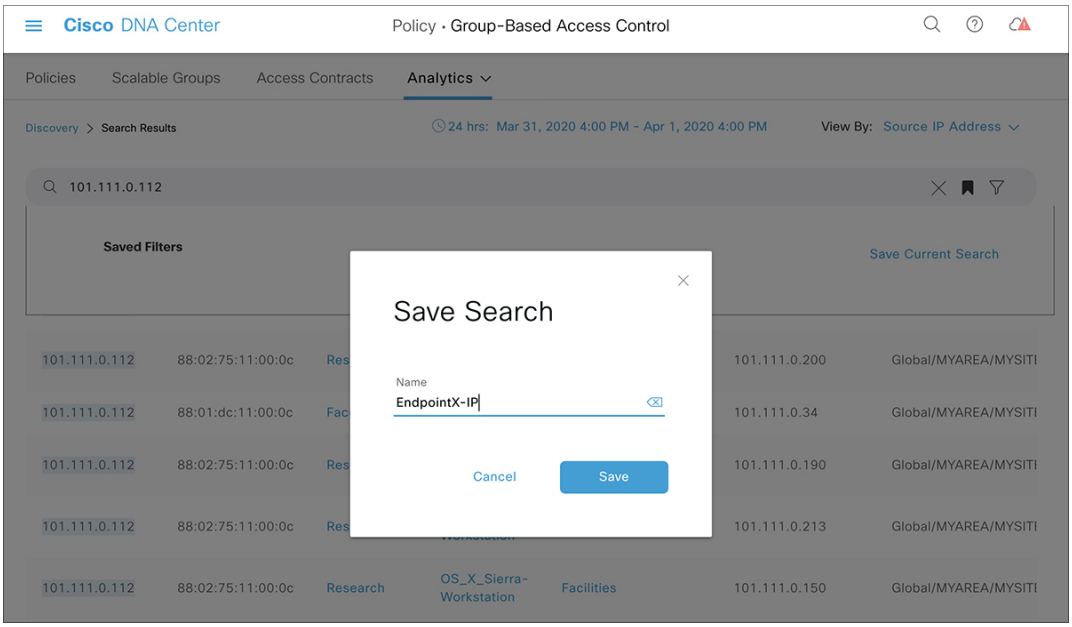
アイコンをクリックして [Save Current Search] オプションを使用すると、現在表示されている検索を保存できます。

図 *25 :* フィルタの保存



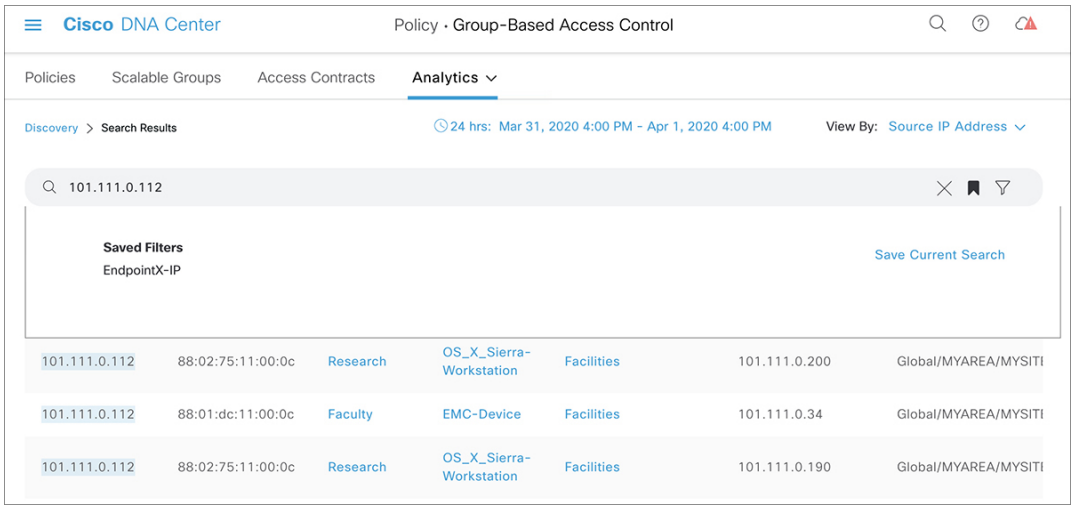
このオプションをクリックした後、検索の名前を入力して保存します。

図 *26 : Save Search*



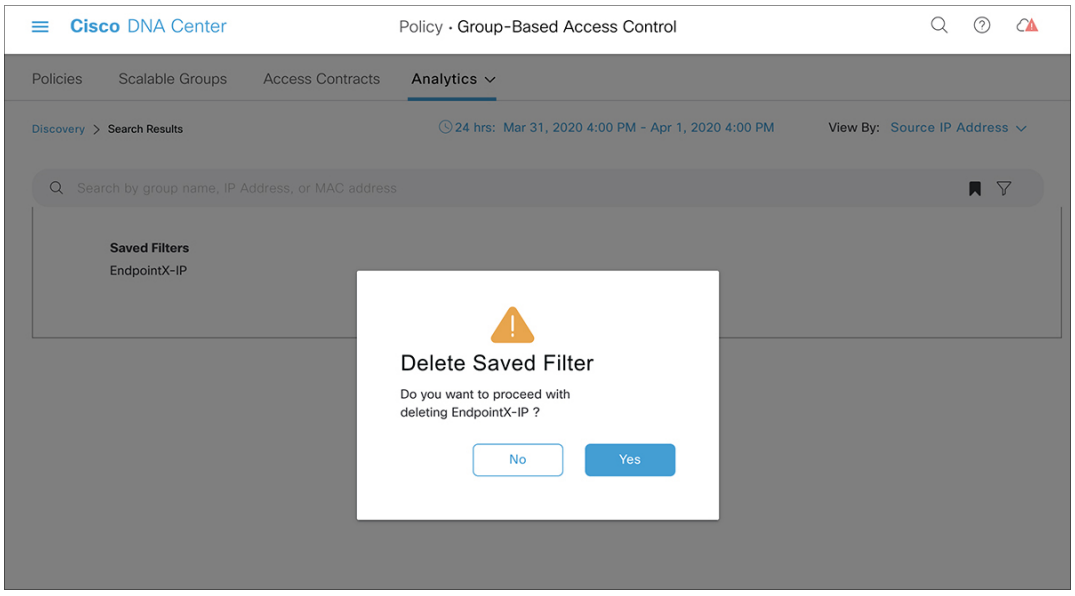
 アイコンをもう一度クリックすると、保存した検索の名前が表示されます。

図 *27* : 保存したフィルタの表示



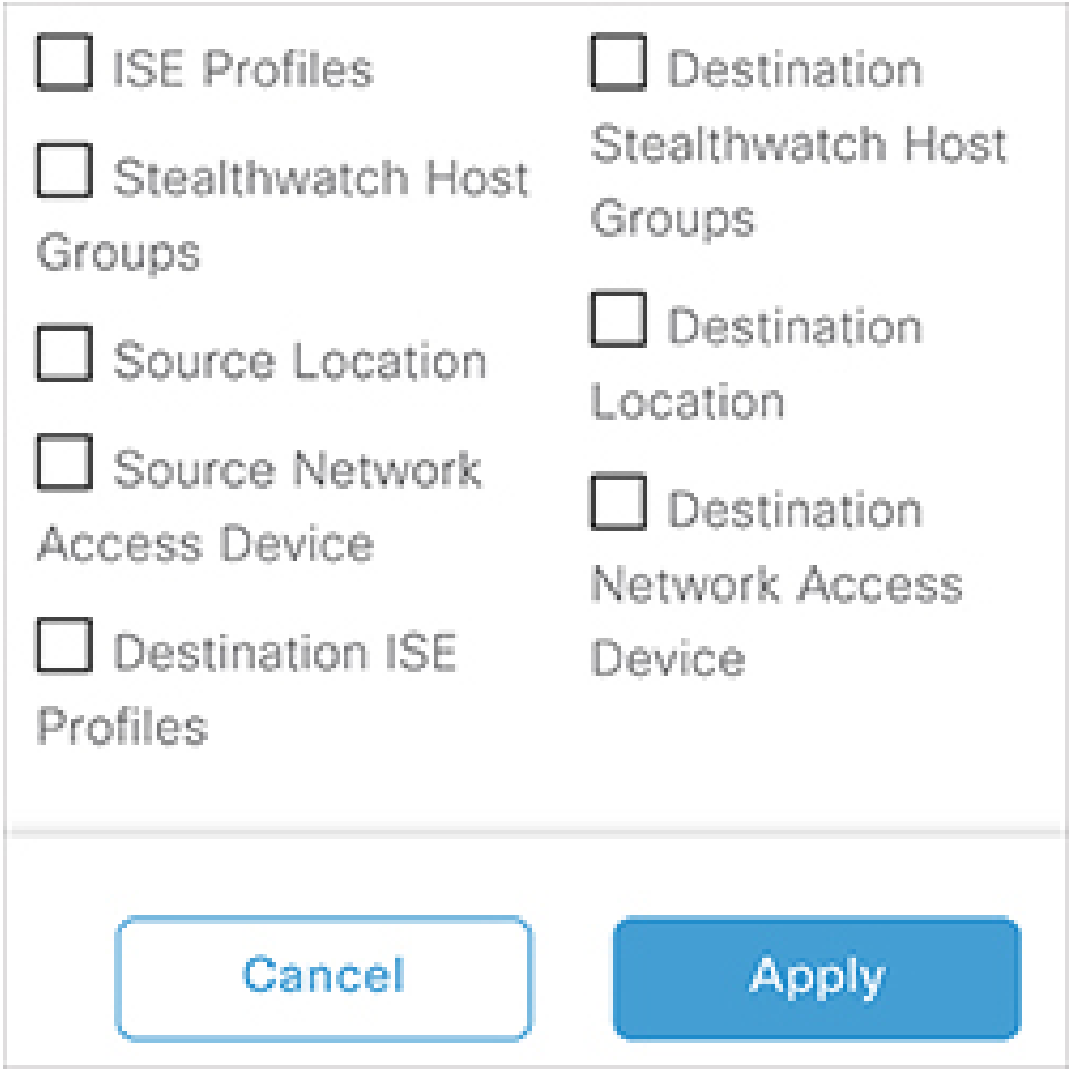
保存した検索を削除するには、  アイコンをクリックします。保存した検索の名前にカーソルを合わせ、  アイコンをクリックします。[Delete Saved Filter] ダイアログボックスで [Yes] をクリックすると、フィルタが完全に削除されます。

図 *28* : 保存したフィルタの削除



7. このアイコンをクリックして列セレクタを開き、検索ビューをカスタマイズします。表示する必要がある列のみを選択して、画面上で目的のデータだけに集中できます。

図 *29 : Column Selector*



8. 1 ページに表示されるレコード数を 1、25、50、100 から選択できます。
9. 前のページまたは次のページがある場合、それに応じて[<]と[>]のリンクが有効になります。

ロールベース アクセス コントロール

シスコのグループベースポリシー分析は、ロールベース アクセス コントロールをサポートしています。読み取り/書き込みユーザーと読み取り専用ユーザーが区別されます。ただし、シスコのグループベースポリシー分析のリリース 1.0 は可視化を主としたもので、システムに変更は加えられないため、読み取り専用ユーザーに対する制限は限られたものになります。

- 読み取り専用ユーザーは検索クエリを保存できません。

- 読み取り専用ユーザーは シスコのグループベースのポリシー分析の初期設定 （21 ページ） ウィンドウで変更を行うことはできません。
- データのエクスポートはHTTPS POST操作であるため、読み取り専用ユーザーはデータをエクスポートできません。
- 読み取り専用ユーザーはグループによる検索のみを実行でき、HTTPS POST操作を伴う他の検索機能は実行できません。

IP ベースのアクセス コントロール ポリシー

IP ベースのアクセス コントロール ポリシーは、アクセス コントロール リスト（ACL）と同じ方法でシスコ デバイスに出入りするトラフィックを制御します。ACL と同様に、IP ベースのアクセス コントロール ポリシーにはプロトコル タイプ、送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号などのさまざまな条件に基づいてトラフィック フローに適用される許可条件および拒否条件のリストが含まれています。

IPベースのアクセスコントロールポリシーを使用して、セキュリティ、モニターリング、ルート選択、ネットワーク アドレス変換などのさまざまな目的のためにトラフィックをフィルタ処理できます。

IPベースのアクセスコントロールポリシーには、次の2つの主要コンポーネントがあります。

- [IP Network Groups]：IP ネットワークグループは、同じアクセス制御要件を共有する IP サブネットで構成されています。これらのグループは Cisco DNA Center でのみ定義できます。IP ネットワークグループに含めることができる IP サブネットは 1 つだけです。
- [Access Contract]：アクセスコントラクトは、IP ベースのアクセス コントロール ポリシーとグループベースのアクセス コントロール ポリシーの両方で使用される共通の構成要素です。これはアクセス制御ポリシーを構成するルールを定義します。これらのルールでは、トラフィックが特定のポートまたはプロトコルに一致したときに実行されるアクション（許可または拒否）や他のルールが一致しないときに実行される暗黙のアクション（許可または拒否）を指定します。

IP ベースのアクセス コントロール ポリシー設定のワークフロー

始める前に

- 新しいIPベースのアクセス コントロール ポリシーを作成中に、**[Policy]** > **[IP Based Access Control]** > **[IP Network Groups]** ウィンドウでグループを追加する場合、Cisco ISE は必須ではありません。
- 次のグローバルネットワーク設定が定義されていることを確認し、デバイスをプロビジョニングします。
  - ネットワークサーバー（AAA、DHCP、DNSサーバーなど）：グローバル ネットワーク サーバーの設定 を参照してください。

- CLI、SNMP、HTTP、HTTPS などのデバイスのログイン情報：グローバル デバイス クレデンシャルについてを参照。
- IP アドレスプール：IP アドレス プールを設定するを参照。
- SSID、ワイヤレスインターフェイス、ワイヤレス無線周波数プロファイルなどのワイヤレス設定：グローバル ワイヤレス設定の構成を参照。
- デバイスのプロビジョニング：プロビジョニングを参照。

ステップ 1 IP ネットワーク グループを作成します。

詳細については、「IP ネットワーク グループの作成 （49 ページ）」を参照してください。

ステップ 2 IP ベースのアクセス制御契約を作成します。

IPベースのアクセス制御契約は、送信元と宛先の間の一連のルールを定義します。これらのルールは、ネットワーク デバイスが、指定されたプロトコルまたはポートに一致するトラフィックに基づいて実行するアクション（許可または拒否）を指定します。詳細については、「IPベースのアクセス コントロール契約の作成 （50 ページ）」を参照してください。

ステップ 3 IP ベースのアクセス コントロール ポリシーの作成アクセス コントロール ポリシーは、送信元と宛先の IP ネットワーク グループ間のトラフィックを制御するアクセス制御契約を定義します。

詳細については、IP ベースのアクセス コントロール ポリシーの作成 （51 ページ）を参照してください。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

ステップ 2 **[DHCP Server]** フィールドに、DHCP サーバーの IP アドレスを入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 3 **[DNS Server]** フィールドに、DNS サーバーのドメイン名を入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 4 [Save] をクリックします。

IP ネットワーク グループの作成

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[IP Based Access Control]** > **[IP Network Groups]** の順に選択します。

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

ステップ 3 **[名前（Name）]** フィールドに、IP ネットワーク グループの名前を入力します。

ステップ 4 **[説明（Description）]** フィールドに、IP ネットワーク グループを説明する単語またはフレーズを入力します。

ステップ 5 **[IP アドレスまたは IP/CIDR（IP Address or IP/CIDR）]** フィールドに、IP ネットワーク グループを構成する IP アドレスを入力します。

ステップ 6 [Save] をクリックします。

IP ネットワーク グループの編集または削除

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[IP Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[IP ネットワーク グループ（IP Network Groups）]** テーブルで、編集または削除するグループの横にあるチェックボックスをオンにします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- グループを変更するには、**[編集（Edit）]**をクリックします。フィールドの定義については、IP ネットワーク グループの作成 （49 ページ） を参照してください。必要な変更を行って、[Save] をクリックします。
- グループを削除するには、**[削除（Delete）]** をクリックし、次に **[はい（Yes）]** をクリックして確定します。

IP ベースのアクセス コントロール契約の作成

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[IP Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 [コントラクトの追加（Add Contract）] をクリックします。

ステップ 3 契約の名前と説明を入力します。

ステップ 4 **[暗黙的アクション（Implicit Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 5 テーブルの **[アクション（Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 6 **[ポート/プロトコル（Port/Protocol）]** ドロップダウン リストから、ポートまたはプロトコルを選択します。

a) Cisco DNA Centerに必要なポートまたはプロトコルがない場合は、**[ポート/プロトコルの追加（Add Port/Protocol）]** をクリックして、自分で作成します。
b) **[名前（Name）]** フィールドで、ポートまたはプロトコルの名前を入力します。
c) [Protocol] ドロップダウンリストから、[UDP]、[TDP]、または [TCP/UDP] を選択します。
d) **[ポート範囲（Port Range）]** フィールドにポート範囲を入力します。
e) Cisco DNA Centerで定義したとおりにポートまたはプロトコルを設定し、競合をレポートしないようにするには、**[競合を無視する（Ignore Conflict）]** チェックボックスをオンにします。
f) **[保存（Save）]** をクリックします。

ステップ 7 （任意） 契約にさらにルールを含めるには、**[追加（Add）]** をクリックして、手順 5 および 6 を繰り返します。

ステップ 8 [Save] をクリックします。

IP ベースのアクセス コントロール ポリシー契約の編集または削除

ポリシーで使用されている契約を編集すると、**[IP ベースのアクセス コントロール ポリシー（IP Based Access Control Policies）]** ウィンドウのポリシーの状態が **[変更（MODIFIED）]** に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[IP Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 契約を変更するには、[編集（Edit）]をクリックして変更を行い、[保存（Save）] をクリックします。フィールドの定義については、IP ベースのアクセス コントロール契約の作成 （50 ページ）を参照してください。

（注） ポリシーで使用されている契約を変更した場合は、**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択し、ポリシー名の横にあるチェックボックスをオンにして、[Deploy] をクリックすることによって、変更したポリシーを展開する必要があります。

- 契約を削除するには、[削除（Delete）] をクリックします。

IP ベースのアクセス コントロール ポリシーの作成

IP ネットワーク グループ間のトラフィックを制限する、IP ベースのアクセス コントロール ポリシーを作成します。

- 1 つのポリシーに異なる設定で複数のルールを追加することができます。
- IP グループと契約の分類子の特定の組み合わせでルールが作成され、デバイスにプッシュされます。この数は、Cisco WLC が ACL でのルールを最大 64 に制限しているため、64 個のルールを超えることはできません。
- **展開された** ポリシー内で使用されるカスタム契約または IP グループが変更された場合、そのポリシーは古いものであり、デバイスにプッシュする新しい設定のために再展開される必要があることを示す [変更済み（Modified）] というステータスでフラグが付けられます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択します。

ステップ 2 [ポリシーの追加（Add Policy）] をクリックします。

ステップ 3 次のフィールドに入力します。

フィールド	説明
Policy Name	ポリシーの名前。
Description	ポリシーを表す単語またはフレーズ。
SSID	SSID の設計中に作成された FlexConnect SSID および 非 FlexConnect SSID をリストします。選択した SSID が FlexConnect モードで設定されている場合、アクセス ポリシーも FlexConnect モードで設定されます。そうでない場合は、通常の方法で設定されます。 （注） SSID が 1 つのポリシーの一部である場合は、その SSID は別のポリシーで使用できません。 ポリシーの展開には有効なサイト SSID の組み合わせが必要です。選択した SSID がデバイスの下でプロビジョニングされていない場合、ポリシーを展開することはできません。

フィールド	説明
Site Scope	サイトのポリシーが適用される範囲。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。詳細については、サイトの範囲 （55 ページ）を参照してください。
Source	契約の影響を受けるトラフィックの送信元。[Source] ドロップダウンリストから、IP ネットワークグループを選択します。使用したい IP ネットワークがない場合は、[+ グループの追加（+Group）] をクリックして作成します。
Contract	ACL 内で送信元と宛先間のネットワーク連携を管理するルール。[契約の追加（Add Contract）] をクリックして、ポリシーの契約を定義します。ダイアログボックスで、使用する契約の横にあるラジオ ボタンをクリックします。または、契約の [許可（permit）]（すべてのトラフィックを許可）または [拒否（deny）]（すべてのトラフィックを拒否）を選択することもできます。
Destination	契約の影響を受けるトラフィックの宛先。[宛先（Destination）] ドロップダウン リストをクリックして、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+ IP ネットワーク グループの作成（+Create IP Network Group）] をクリックして作成します。
Direction	送信元と宛先間のトラフィック フローの関係を設定します。送信元から宛先へのトラフィック フローの契約を有効にするには、[一方向（One-Way）] を選択します。両方向（送信元から宛先へ、および宛先から送信元へ）でのトラフィック フローの契約を有効にするには、[双方向（Bi-directional）] を選択します。

ステップ 4 （任意） IP ネットワーク グループを作成するには、[IP ネットワーク グループの作成（Create IP Network Group）] をクリックします。

ステップ 5 （任意） 別のルールを追加するには、プラス記号をクリックします。

（注） ルールを削除するには、[x] をクリックします。

ステップ 6 （任意） ルールの順序を変更するには、変更したい順序でルールをドラッグ アンド ドロップします。

ステップ 7 [Deploy] をクリックします。

「IP ベースのアクセス コントロール ポリシーが作成され、正常に展開されました」という成功メッセージが表示されます。選択した SSID によっては、FlexConnect ポリシーまたは標準ポリシーが異なるマッピング情報レベルで作成され、展開されます。ポリシーの [ステータス（Status）] は、[展開済み（DEPLOYED）] として表示されます。[ポリシー名（Policy Name）] の横にあるワイヤレス アイコンは、展開されたアクセス ポリシーがワイヤレス ポリシーであることを示しています。

IP ベースのアクセス コントロール ポリシーの編集または削除

必要な場合は、IP ベースのアクセス コントロール ポリシーを変更または削除できます。

（注） ポリシーを編集すると、[IPベースのアクセスコントロールポリシー（IP-Based Access Control Policies）] ウィンドウのポリシーの状態が [変更（MODIFIED）] に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択します。

ステップ 2 編集または削除するポリシーの横にあるチェック ボックスをオンにして、次のいずれかのタスクを実行します。

- 変更するには、[編集（Edit）]をクリックします。完了したら、[Save]をクリックします。フィールドの定義については、IP ベースのアクセス コントロール ポリシーの作成 （51 ページ）を参照してください。
- ポリシーを削除するには、**[削除（Delete）]** をクリックします。

ステップ 3 ポリシーを変更した場合は、ポリシー名の横にあるチェック ボックスをオンにして [展開（Deploy）] をクリックすることによって、変更したポリシーを展開します。

IP ベースのアクセス コントロール ポリシーの展開

ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再度展開する必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択します。

ステップ 2 展開するポリシーを探します。

ステップ 3 ポリシーの横にあるチェック ボックスをオンにします。

ステップ 4 [Deploy] をクリックします。
ポリシーを今すぐ展開するか、または後でスケジュールするかどうかを求められます。

ステップ 5 次のいずれかを実行します。

- ポリシーをすぐに展開するには、**[今すぐ実行（Run Now）]** ラジオ ボタンをクリックし、**[適用（Apply）]** をクリックします。
- 将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーション ポリシー

Quality of Service（QoS）とは、選択したネットワーク トラフィックに、優先的なサービスやニーズに合ったサービスを提供するネットワーク機能を意味します。QoS を設定することで、ビジネスの目標（音声品質が会社の標準規格を満たしていることの保証、ビデオの高い Quality of Experience（QoE）の確保など）を引き続き順守しながら、ネットワーク リソースを最も効率的に使用する方法でネットワーク トラフィックを処理することができます。

QoS は、Cisco DNA Center のアプリケーション ポリシーを使用してネットワークに設定できます。アプリケーション ポリシーは、次の基本的なパラメータで構成されています。

- [Application Sets]：同様のネットワークトラフィックを必要とする一連のアプリケーション。各アプリケーションセットには、トラフィックの優先順位を定義するビジネスとの関連性グループ（ビジネス関連、デフォルト、またはビジネスと無関係）が割り当てられます。QoS パラメータは、Cisco Validated Design（CVD）に基づいて 3 つのグループごとに定義されます。一部のパラメータは、それぞれの目的に合わせてより詳細に調整できます。
- [Site Scope]：アプリケーションポリシーが適用されているサイト。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。

Cisco DNA Center はこれらのパラメータをすべて受け取り、適切なデバイスの CLI コマンドに変換します。Cisco DNA Center はポリシーの展開時に、サイトの範囲で定義されているデバイスに各コマンドを設定します。

（注） Cisco DNA Center はデバイスで使用可能な QoS 機能セットに基づいて、各デバイスに QoS ポリシーを設定します。デバイスの QoS 実装の詳細については、対応するデバイスの製品マニュアルを参照してください。

アプリケーション ポリシーでの CVD ベースの設定

アプリケーション ポリシーのデフォルトの QoS 信頼およびキューイング設定は、Enterprise Medianet の QoS デザイン向けの Cisco Validated Design（CVD）に基づいています。CVD は、一般的な使用例や現行のシステム設計上の優先事項に基づき、システム設計の基盤を提示しています。CVD には、お客様のニーズに応じるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。それぞれのソリューションには、エンジニアによる包括的なテ

ストと文書化が実施されており、迅速で、信頼性が高く、予測可能な導入が確保されています。

QoS に関連する最新の検証済み設計は、Cisco Press の書籍『*End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition』（http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694）で公開されています。追加情報については、次のシスコのドキュメントを参照してください。

- シスコ検証済みデザイン（CVD）
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

サイトの範囲

サイト範囲は、アプリケーションポリシーが適用されるサイトを定義します。ポリシーを定義するときに、ポリシーが有線デバイス用かワイヤレスデバイス用かを設定します。また、サイト範囲も設定します。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、サイト範囲内で SSID が定義されている、サイト範囲内のすべてのワイヤレス デバイスにポリシーが適用されます。

これにより、有線ネットワーク セグメントとワイヤレス ネットワークセグメントの動作の相違を補うために、必要に応じてトレードオフを実施できます。たとえば、ワイヤレス ネットワークでは通常、有線ネットワークと比較した場合に低帯域幅、低速、パケット損失増加の特徴があります。個々のワイヤレスセグメントは、ローカルの RF 干渉、輻輳、ネットワーク デバイスの機能の違いなどの要因によってさらに変動が見られます。個々のワイヤレスセグメントにセグメントごとのポリシーを適用できるすることで、優先順位の高いトラフィックが受ける、ワイヤレス ネットワークの劣化による影響が小さくなるように、トラフィック処理ルールを調整できます。

ビジネス関連のグループ

ビジネス関連グループは、ビジネスや事業への関連性に応じて、指定されたアプリケーション セットを分類します。

ビジネス関連グループ（ビジネス関連、デフォルト、ビジネスと無関係）は、基本的に 3 種類のトラフィック（高優先順位、ニュートラル、低優先順位）にマッピングされます。

- **ビジネス関連（Business Relevant）**：（高優先トラフィック）このグループのアプリケーションは組織の目的に直接関与し、音声、ビデオ、ストリーミング、コラボレーション型マルチメディア アプリケーション、データベース アプリケーション、エンタープライズ リソース アプリケーション、電子メール、ファイル転送、コンテンツ配布など、さまざまな種類があります。ビジネス関連として指定されているアプリケーションは、Internet

Engineering Task Force（IETF）RFC 4594 の規定に従い、業界推奨のベスト プラクティスに従って処理されます。

- **デフォルト（Default）**：（平均的優先度のトラフィック）このグループは、ビジネスに関連している場合もあればしていない場合もあるアプリケーションを対象としています。たとえば一般的な HTTP または HTTPS トラフィックは、組織の目的に寄与する場合もしない場合もあります。たとえば、レガシーアプリケーションや新しく導入されたアプリケーションなどでも、一部のアプリケーションの目的については分析していない場合があります。したがって、これらのアプリケーションのトラフィック フローは、IETF RFC 2747 および 4594 で説明されているように、デフォルトの転送サービスで処理する必要があります。
- **ビジネスと無関係（Business Irrelevant）**：（低優先トラフィック）このグループは、組織の目的達成に寄与しないと識別されたアプリケーションを対象としています。主にコンシューマ向けかエンターテイメント向け、あるいは本質的にその両方に該当するアプリケーションです。この種類のトラフィックは、IETF RFC 3662 および 4594 で説明されている「スカベンジャ」サービスとして処理することをお勧めします。

アプリケーションはアプリケーションセットに分類されて、ビジネス関連グループにソートされます。アプリケーションセットはポリシーに現状のまま含めることができます。または、ビジネス目標やネットワーク構成のニーズを満たすように変更することができます。

たとえば、YouTube はコンシューマ メディア アプリケーション セットのメンバーです。一般的に、ほとんどのお客様がこのアプリケーションをこのように分類しているため、（デフォルトでは）YouTubeはビジネスと無関係です。ただし、この分類がすべての企業に当てはまるわけではありません。たとえば、いくつかのビジネスでは YouTube をトレーニング目的で使用することがあります。このような場合、管理者は、デフォルトでビジネス関連であるストリーミング ビデオ アプリケーション セットに YouTube アプリケーションを移動できます。

コンシューマとプロデューサ

あるアプリケーションから別のアプリケーションにトラフィックが送られた（特定の a から b へのトラフィック フローが作成された）ときにトラフィックが特定の方法で処理されるように、アプリケーション間の関係を設定することができます。このような関係のアプリケーションをプロデューサとコンシューマと呼び、次のように定義しています。

- **プロデューサ**：アプリケーション トラフィックの送信元。たとえば、クライアント/サーバー アーキテクチャでは、トラフィック フローは主にサーバーからクライアントの方向であるため、アプリケーション サーバーがプロデューサと見なされます。ピアツーピア アプリケーションの場合は、リモート ピアがプロデューサと見なされます。
- **コンシューマ**：アプリケーション トラフィックの受信者。コンシューマに該当するのは、クライアント/サーバー アーキテクチャの場合はクライアント エンドポイント、ピアツーピア アプリケーションの場合はローカル デバイスなどです。コンシューマはエンドポイント デバイスであることがありますが、場合によっては、そのようなデバイスの特定のユーザーであることもあります（通常、IPアドレスまたは特定のサブネットによって識別

される）。また、あるアプリケーションが別のアプリケーション トラフィック フローのコンシューマになる場合もあります。

このような関係を設定することにより、このシナリオに一致するトラフィックに特定のサービス レベルを設定することが可能になります。

マーキング、キューイング、ドロッピングの処理

Cisco DNA Center は、IETF RFC 4594 およびアプリケーションに割り当てられたビジネス関連のカテゴリでの処理のマーキング、キューイング、およびドロッピングをベースとしています。Cisco DNA Center は、デフォルト カテゴリのすべてのアプリケーションをデフォルトの転送アプリケーション クラスに割り当て、無関係なビジネス カテゴリのすべてのアプリケーションをスカベンジャ アプリケーション クラスに割り当てます。関連するビジネス カテゴリのアプリケーションについては、Cisco DNA Center はアプリケーションのタイプに基づいてトラフィック クラスをアプリケーションに割り当てます。次の表に、アプリケーション クラスとそれぞれの処理を示します。

表 *3:* マーキング、キューイング、ドロッピングの処理

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロッピング	アプリケーションの説明
該当する	VoIP[1]	Expedited Forwarding（EF）	プライオリティキューイング（PQ）	VoIP テレフォニー（ベアラのみ）トラフィック。たとえば、Cisco IP 電話。
	ブロードキャストビデオ	クラス セレクタ（CS）5	PQ	ブロードキャスト TV、ライブイベント、ビデオ監視フロー、同様の非弾性ストリーミング メディア フロー（Cisco IP Video Surveillance や Cisco Enterprise TV など）。（非弾性フローとは、非常にドロップされやすく、再送信またはフロー制御機能のいずれか、または両方がないフローを意味します。）
	リアルタイムインタラクティブ	CS4	PQ	非弾性の高解像度インタラクティブ ビデオ アプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco TelePresence など）。
	マルチメディア会議	相対的優先転送（AF）41	帯域幅（BW）キューと Differentiated Services Code Point（DSCP）Weighted Random Early Detect（WRED）	デスクトップソフトウェアのマルチメディア コラボレーションアプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco Jabber や Cisco WebEx など）。
	マルチメディア ストリーミング	AF31	BW キューと DSCP WRED	ビデオオンデマンド（VoD）ストリーミング ビデオフローおよび仮想デスクトップアプリケーション。たとえば、Cisco Digital Media System。
	ネットワーク制御	CS6	BW キューのみ[2]	EIGRP、OSPF、BGP、HSRP、IKE などのエンタープライズネットワークの信頼性の高い運用のために必要とされるネットワーク コントロール プレーン トラフィック。
	シグナリング	CS3	BW キューと DSCP	IP 音声およびビデオ テレフォニー インフラストラクチャのコントロールプレーン トラフィック。
	Operations, Administration, and Management（OAM）	CS2	BW キューと DSCP[3]	SSH、SNMP、syslog などのネットワーク運用、管理、管理トラフィック
		AF21		

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロッピング	アプリケーションの説明
	トランザクションデータ（低遅延データ）		BW キューと DSCP WRED	エンタープライズ リソース プランニング（ERP）、顧客関係管理（CRM）、およびその他のデータベース アプリケーションなどのインタラクティブ（フォアグラウンド）データ アプリケーション。
	バルクデータ（高スループットデータ）	AF11	BW キューと DSCP WRED	電子メール、File Transfer Protocol（FTP）、バックアップ アプリケーションなどの非インタラクティブ（バックグラウンド）データ アプリケーション。
デフォルト	デフォルトの転送（ベストエフォート）	DF	デフォルト キューと RED	デフォルトのアプリケーション、およびデフォルトのビジネス関連グループに割り当てられるアプリケーション。プライオリティ、保証された帯域幅、または差分サービス クラスに割り当てられるのはごく少数のアプリケーションであるため、大部分のアプリケーションは引き続きデフォルトでベストエフォート型サービスになります。
非関連	スカベンジャー	CS1	最小 BW キュー（ディファレンシャル）と DSCP	非ビジネス関連のトラフィック フロー、およびビジネス関連でないグループに割り当てられているアプリケーション（エンターテイメント向けのデータやメディア アプリケーションなど）。たとえば、YouTube、Netflix、iTunes、Xbox Live。

[1] VoIP シグナリング トラフィックは、コール シグナリング クラスに割り当てられます。
[2] ネットワーク制御トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。
[3] OAM トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

サービス プロバイダのプロファイル

サービス プロバイダ（SP）プロファイルは、特定の WAN プロバイダのサービス クラスを定義します。4 クラス、5 クラス、6 クラス、8 クラスのモデルを定義できます。

アプリケーション ポリシーがデバイスに展開されると、各 SP プロファイルには、各 SP クラスを DSCP 値と帯域幅割り当てのパーセンテージにマップする特定のサービス レベル契約（SLA）が割り当てられます。

アプリケーション ポリシーを設定するときに SP プロファイルの DSCP 値と 帯域幅割り当てのパーセンテージをカスタマイズできます。

SPプロファイルを作成したら、そのプロファイルをWANインターフェイスで設定する必要があります。

表 *4:4* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
デフォルト	0	—	—	31

表 *5:5* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
クラス 3 データ	AF11	—	—	1
デフォルト	ベストエフォート	—	—	30

表 *6:6* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
クラス 1 データ	AF31	—	—	10
クラス 3 データ	AF11	—	—	1
ビデオ	AF41	—	—	34
音声	EF	はい	10	—
デフォルト	0	—	—	30

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
クラス 2 データ	AF21	—	—	25

表 *7:8* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
ネットワーク-コントロール管理	CS6	—	—	5
ストリーミング ビデオ	AF31	—	—	10
コール シグナリング	CS3	—	—	4
スカベンジャー	CS1	—	—	1
インタラクティブ ビデオ	AF41	—	—	30
音声	EF	はい	10	—
デフォルト	0	—	—	25
重要なデータ	AF21	—	—	25

キューイング プロファイル

キューイング プロファイルでは、インターフェイス速度とトラフィック クラスに基づいたインターフェイスの帯域幅割り当てを定義することができます。

（注） キューイングプロファイルは、サービス プロバイダ プロファイルに接続されている WAN 側インターフェイスには適用されません。

次のインターフェイス速度がサポートされます。

- 100 Gbps
- 10/40 Gbps
- 1 Gbps

- 100 Mbps
- 10 Mbps
- 1 Mbps

インターフェイスの速度が 2 つのインターフェイス速度の間である場合、Cisco DNA Center は、より低いインターフェイス速度でインターフェイスを取り扱います。

（注） Cisco DNA Center は、正しいポリシーを適用するためにインターフェイスの動作速度の検出を試みます。ただし、スイッチ ポートが管理上ダウンしている場合、Cisco DNA Center は速度を検出できません。この場合、Cisco DNA Center は、インターフェイスのサポートされた速度を使用します。

キューイング ポリシーは、アプリケーション ポリシーの一部として定義します。アプリケーションポリシーを展開すると、サイト範囲内の選択されたサイトのデバイスが、割り当てられた LAN キューイング ポリシーで設定されます。LAN キューイング ポリシーが割り当てられていない場合、アプリケーション ポリシーはデフォルトの CVD キューイング ポリシーを使用します。

すでに展開されているアプリケーション ポリシーのキューイング ポリシーを変更すると、ポリシーは失効し、変更をデバイスに適用するにはポリシーを展開しなおす必要があります。

キューイング ポリシーに関する次の追加の注意事項および制約事項に注意してください。

- LANキューイングプロファイルは、ポリシーで使用されている場合には削除できません。
- ポリシーに関連付けられているキューイングプロファイルを更新すると、ポリシーは期限切れとしてマーキングされます。最新の変更をプロビジョニングするには、ポリシーを展開しなおす必要があります。
- トラフィック クラス キューイングをカスタマイズしても、シスコのサービス プロバイダ スイッチおよびルータのインターフェイスは影響を受けません。これらのインターフェイスの設定は、引き続き Cisco DNA Center を使用することなく実施します。

表 *8:* デフォルト *CVD LAN* キューイング ポリシー

トラフィック クラス	デフォルトの帯域幅（合計= 100%）[4]
ビジネス関連の音声	10%
ビジネス関連のブロードキャストビデオ	10%
ビジネス関連のリアルタイム インタラクティブ	13%
ビジネス関連のマルチメディア会議	10%

トラフィック クラス	デフォルトの帯域幅（合計= 100%）[4]
ビジネス関連のマルチメディア ストリーミング	10%
ビジネス関連のネットワーク制御	3%
ビジネス関連のシグナリング	2%
ビジネス関連の OAM	2%
ビジネス関連のトランザクションデータ	10%
ビジネス関連のバルクデータ	4%
ビジネス関連のスカベンジャ	1%
ビジネス関連のベストエフォート	25%

[4] 音声、ブロードキャストビデオ、およびリアルタイムインタラクティブ トラフィック クラスの合計帯域幅を 33% 以下にすることを推奨します。

リソースが制限されているデバイスの処理順

ネットワーク デバイスの中には、ネットワーク アクセス コントロール リスト（ACL）および ACE を格納するためのメモリ（TCAM と呼ばれる）が制限されているものがあります。このため、アプリケーション用の ACL と ACE がこれらのデバイス上に設定されている場合は、利用可能な TCAM 領域が使用されます。When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

そのようなデバイスで最も重要なアプリケーションの QoS ポリシーが確実に設定されるように、Cisco DNA Center は次の順序で TCAM スペースを割り当てます。

1. [Rank]：カスタムアプリケーションおよびお気に入りのアプリケーションに割り当てられた番号（ただし既存のデフォルト NBAR アプリケーションは除く）。ランクの番号が小さくなるほど、優先順位が高くなります。たとえば、ランク 1 のアプリケーションはランク 2 のアプリケーションよりも優先順位が高くなります。ランクがない場合は、優先順位が最も低くなります。

（注）
- カスタム アプリケーションには、デフォルトでランク 1 が割り当てられています。
- NBAR アプリケーションをお気に入りとしてマークすると、ランクは 1000 に設定されます。

2. [Traffic Class]：優先順位は次の順序に基づいています。シグナリング、バルクデータ、ネットワーク制御、Operations Administration Management（Ops Admin Mgmt）、トランザクショ

ンデータ、スカベンジャ、マルチメディアストリーミング、マルチメディア会議、リアルタイム インタラクティブ、ブロードキャストビデオ、VoIP テレフォニー。

3. [Popularity]：CVD の基準に基づいて割り当てられた番号（1 ～ 10）。ポピュラリティの番号は変更できません。ポピュラリティが 10 のアプリケーションは、ポピュラリティが 9 のアプリケーションよりも優先順位が高くなります。

（注）
- カスタムアプリケーションには、ポピュラリティ 0 が割り当てられます。
- デフォルトNBARアプリケーションには、CVDの基準に基づいてポピュラリティ番号（1 ～10）が割り当てられます。アプリケーションをお気に入りとしてマークしても、ポピュラリティ番号は変わりません（ランクのみ変更されます）。

4. [Alphabetization]：2 つ以上のアプリケーションのランクとポピュラリティ番号が同一の場合、それらのアプリケーションはアプリケーション名のアルファベット順にソートされ、ソート順に従い優先順位が割り当てられます。

たとえば、次のアプリケーションを指定したポリシーを定義する場合を想定しましょう。

- カスタム アプリケーション custom_realtime。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- カスタム アプリケーション custom_salesforce。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- corba-iiop という名前のトランザクション データ トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 9 が付与されています。
- gss-http という名前の Ops Admin Mgmt トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 10 が付与されています。
- 他のすべてのデフォルトNBARアプリケーションにはランクはありませんが、トラフィック クラスと（CVD に基づいて）デフォルト ポピュラリティに従って処理されます。

優先順位付けのルールに従って、アプリケーションはデバイスにおいて次の順序で設定されます。

アプリケーションの設定順	理由
1. カスタム アプリケーション custom_realtime	カスタム アプリケーションには最も高い優先順位が付与されます。custom_salesforce アプリケーションと custom_realtime アプリケーションのランクおよびポピュラリティが同じであるとすると、これらのアプリケーションはアルファベット順にソートされ、custom_realtime が custom_salesforce より前になります。
2. カスタム アプリケーション custom_salesforce	

アプリケーションの設定順	理由
3. お気に入りのアプリケーション gss-http	これら両方のアプリケーションはお気に入りとして指定されているため、同じアプリケーション ランクになります。そのため、Cisco DNA Center は各アプリケーションをトラフィック クラスに基づいて評価します。gss-http は、Ops Admin Mgmt トラフィック クラスであるため、先に処理され、その後にトランザクションデータ トラフィック クラスの corba-iiop アプリケーションが処理されます。トラフィック クラスによって処理順が決まっているため、ポピュラリティは考慮されません。
4. お気に入りのアプリケーション corba-iiop	
5. 他のすべてのデフォルト NBAR アプリケーション	他のすべてのアプリケーションは、トラフィック クラスとポピュラリティに従って次に優先され、ポピュラリティが同じアプリケーションは、アプリケーション名のアルファベット順にソートされます。

ポリシーのドラフト

ポリシーを作成するときに、ポリシーを展開せずにドラフトとして保存できます。ドラフトとして保存すると、後でポリシーを開いて変更できます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

（注） ポリシーを保存または展開した後に、名前を変更することはできません。

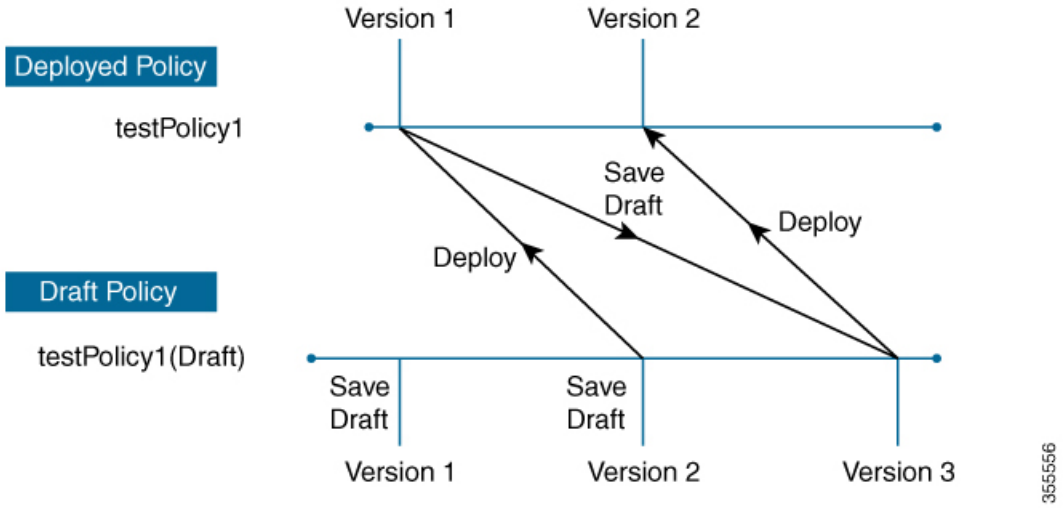
ドラフトポリシーと展開したポリシーは相互に関連付けられますが、それぞれ独自にバージョン管理されます。

ポリシーをドラフトとして保存すると、Cisco DNA Center はポリシー名に (Draft) を追加してバージョン番号を 1 つ上げます。ポリシーを展開すると、Cisco DNA Center が展開したポリシーのバージョン番号を 1 つ上げます。

たとえば、次の図に示すように、testPolicy1 という名前のポリシーを作成してドラフトとして保存します。ポリシーは testPolicy1 (Draft)、バージョン番号 1 として保存されます。ドラフトを変更して、再度保存します。ポリシーの名前は同じ testPolicy1 (Draft) のままですが、バージョン番号は 2 に上がります。

ポリシーが気に入ったのでネットワークに展開します。ポリシーは testPolicy1 という名前で展開され、バージョン番号は 1 です。展開したポリシーを変更して、ドラフトとして保存します。ドラフトポリシー testPolicy1 (Draft) は、バージョン番号 3 に上がります。最終的にそのバージョンを展開するとき、testPolicy1 はバージョン 2 になります。

図 *30* : 展開したポリシーとドラフト ポリシーのバージョン管理



ドラフトポリシーまたは展開したポリシーのいずれかを変更および保存するときは、ドラフトポリシーのバージョン番号が上がります。同様に、ドラフトポリシーまたは変更した展開済みポリシーのいずれかを展開するときは、展開したポリシーのバージョンが上がります。

展開したポリシーと同様に、ドラフト ポリシーの履歴を表示し、以前のバージョンにロールバックすることができます。

ポリシー バージョンの履歴表示と以前のバージョンへのロール バックについては、ポリシーのバージョン管理 （67 ページ）を参照してください。

ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用される CLI を生成できます。

プレビュー操作では、ポリシーのCLIコマンドが生成され、デバイスの実行コンフィギュレーションのCLIコマンドと比較され、デバイスでポリシーを設定するのに必要な残りのCLIだけが返されます。

プレビュー出力の確認後、範囲内の全デバイスにポリシーを展開するか、ポリシーの変更を続行することができます。

ポリシーの事前チェック

アプリケーションポリシーを作成するとき、ポリシーを展開する前に、サイト範囲のデバイスでサポートされるかどうかを確認できます。事前チェック機能では、デバイス タイプ、モデル、ライン カード、およびソフトウェア イメージが作成したアプリケーション ポリシーをサポートするかどうかチェックします。これらのコンポーネントのいずれかがサポートさCisco DNA Centerれていない場合、はデバイスの障害を報告します。Cisco DNA Centerまた、障害を修正する方法についても説明します。これらの対応で障害が修正されない場合、サイト範囲からデバイスを削除できます。

アプリケーション ポリシーをそのまま展開すると、事前チェック プロセス中に障害が報告されたデバイスでポリシー展開が失敗します。失敗を回避するには、サイト範囲からデバイスを削除するか、デバイス コンポーネントをアプリケーション ポリシーがサポートするレベルに更新します。サポート対象デバイスのリストについては、Cisco DNA Center のサポート対象デバイスドキュメントを参照してください。

ポリシーのスケジューリング

ポリシーを作成または変更した後に、そのポリシーを、ポリシーに関連付けられたデバイスに展開または再展開できます。このポリシーの展開/再展開は、すぐに行うことも、特定の日時（たとえば、週末のオフピーク時）に行うこともできます。ポリシー導入のスケジューリングは有線またはワイヤレスのデバイスに対して実施できます。

展開するポリシーのスケジュールを設定すると、そのポリシーとサイト範囲がロックされます。ポリシーの表示は可能ですが、編集することはできません。ポリシーを展開する予定が変更された場合は、その展開をキャンセルできます。

（注） スケジュール イベントが発生すると、ポリシーは、さまざまなポリシー コンポーネント（アプリケーション、アプリケーションセット、およびキューイング プロファイルなど）に対して検証されます。この検証に失敗すると、ポリシーの変更は行われません。

ポリシーのバージョン管理

このポリシーのバージョン管理により、次のタスクが可能になります。

- 以前のバージョンと現在（最新）のバージョンを比較して相違点を確認する。
- ポリシーの以前のバージョンを表示し、サイト範囲内のデバイスに再適用するバージョンを選択する。

あるバージョンのポリシーを編集しても、そのポリシーの別のバージョンやポリシーのコンポーネント（そのポリシーによって管理されるアプリケーションセットなど）は影響を受けません。たとえば、ポリシーからアプリケーションセットを削除しても、そのアプリケーションセットは Cisco DNA Center、そのポリシーの別のバージョン、または他のポリシーからは削除されません。ポリシーとアプリケーションセットは互いに独立して存在するため、存在しなくなったアプリケーションセットを含むバージョンのポリシーを保持できます。存在しなくなったアプリケーションセットを参照するポリシーを展開しようとしたり、それらのポリシーを古いバージョンにロールバックしようとしたりすると、エラーが発生します。

（注） ポリシーのバージョン管理では、アプリケーション（ランク、ポート、プロトコルなど）、アプリケーション セット メンバー、LAN キューイング プロファイル、およびサイトの変更は取得されません。

オリジナルポリシーの復元

初めてデバイスにポリシーを展開する際、Cisco DNA Centerは、デバイスの元のCisco Modular QoS CLIポリシー設定をデタッチしますが、それらはデバイス上に残ります。Cisco DNA Centerは、デバイスの元のNBAR設定をCisco DNA Centerに保存します。このアクションにより、必要に応じてオリジナルのモジュラー式QoS CLIポリシーとNBAR設定を後でデバイスに復元することが可能になります。

（注） このようにモジュラー式QoS CLIポリシーはデバイスから削除されませんが、ユーザーがこれらのポリシーを削除すると、元のポリシー復元するCisco DNA Centerの機能を使用してそれらを復元することができなくなります。

元のポリシー設定をデバイスに復元する際、Cisco DNA Centerは、展開されている既存のポリシー設定を削除し、デバイス上にあった元の設定に戻します。

アプリケーション ポリシーを展開する前に存在していたモジュラー式QoS CLIポリシー設定はすべて、インターフェイスに再アタッチされます。ただし、マルチレイヤ スイッチング（MLS）設定などのキューイング ポリシーは復元されません。代わりに、デバイスは、Cisco DNA Centerによって最後に適用されたMLS設定を維持します。

元のポリシー設定をデバイスに復元すると、Cisco DNA Centerに保存されているポリシーが削除されます。

この機能には、次のような追加のガイドラインと制限事項があるので、注意してください。

- 初めてポリシーをデバイスに展開する試みが失敗すると、Cisco DNA Centerは、元のポリシー設定をデバイスに復元することを自動的に試みます。
- そのポリシーがデバイスに適用された後にデバイスがアプリケーションポリシーから削除された場合、そのポリシーはデバイス上に残ります。Cisco DNA Centerは、ポリシーを自動的に削除したり、デバイスのQoS設定を元の(事前Cisco DNA Center)設定に復元したりしません。

陳腐化したアプリケーション ポリシー

ポリシーで参照されているものの設定を変更すると、アプリケーションポリシーが陳腐化する可能性があります。アプリケーションポリシーが陳腐化した場合、変更を有効化するためにアプリケーション ポリシーを再展開する必要があります。

アプリケーション ポリシーは、次の理由で陳腐化する可能性があります。

- アプリケーション設定で参照されているアプリケーションの変更。
- SPプロファイルの割り当て、WANサブ回線のレート、WANまたはLANマーキングなどのインターフェイスの変更。
- キューイング プロファイルの変更。

- ポリシーの親サイト下への新規サイトの追加。
- ポリシーによって参照されるサイトへのデバイスの追加。
- ポリシーが同じサイト間でのデバイスの移動。
- インターフェイス除外/包含の変更。
- デバイスコントローラベースのアプリケーション認識（CBAR）ステータスの変更。

アプリケーション ポリシーのガイドラインと制限事項

- Cisco DNA Center は、ワイヤレスコントローラ上で同じ SSID 名を使用して複数の WLAN を学習できません。WLC には、名前は同じで WLAN プロファイル名が異なる複数のエントリを含めることもできますが、Cisco DNA Center はどの時点においても、一意の名前を持つ WLAN に対するエントリを 1 つだけ持ちます。

  WLC ごとに重複する SSID 名を意図的に持つことも、Cisco DNA Center を使用して重複する SSID 名を持つ WLC を誤って追加してしまうこともあります。いずれの場合も、WLC ごとに重複する SSID 名を持つことは一部の機能にとって問題になります。

  - [Learn Config]：Cisco DNA Center は WLC ごとにランダムに選択された 1 つの SSID 名のみ学習し、残りの重複する SSID 名はすべて破棄します。（[設定の学習（Learn Config）] は、通常はブラウンフィールド シナリオで使用されます）。
  - [Application Policy]：Cisco DNA Center は、アプリケーションポリシーの展開時に、重複するいずれかの SSID 名にのみポリシーをランダムに適用して、他には適用しません。さらに、ポリシーの復元、CLI プレビュー、EasyQoS ファーストレーン、および PSK オーバーライド機能が失敗するか、予期しない結果が生じることになります。
  - [Multiscale Network]：MULTISCALE ネットワークでは、複数のデバイスの複数の重複する SSID 名が原因で問題が発生することがあります。たとえば、1 台のデバイスには非ファブリック SSID として WLAN が設定されていて、2 台目のデバイスには同じ WLAN がファブリック SSID として設定されている場合、[設定の学習（Learn Config）] を実行すると、1 つの SSID 名のみ学習されます。その他のデバイスの他の SSID 名は破棄されます。この動作により、特に、2 台目のデバイスがファブリック SSID 名のみサポートしていて、Cisco DNA Center が非ファブリック SSID 名を持つデバイスに対して操作を実行しようとする場合に競合が生じることがあります。
  - [IPACL Policy]：Cisco DNA Center は、IPACL ポリシーの展開時に、重複する SSID のいずれか 1 つにのみランダムにポリシーを適用します。また、Flex Connect が関係するシナリオも影響を受けます。

- Cisco DNA Center では、デバイス設定に対するアウト オブ バンド（OOB）の変更は推奨されません。OOB に変更を加えると、Cisco DNA Center のポリシーとデバイスに設定されているポリシーは一貫性のない状態になります。2 つのポリシーは、Cisco DNA Center のポリシーをデバイスに再度展開するまで一貫性のない状態のままになります。
- QoS trust 機能は変更できません。

- ワイヤレスコントローラではカスタムアプリケーションはサポートされていません。したがって、ワイヤレス アプリケーション ポリシーの作成時にはカスタムアプリケーションは選択されません。
- 設計から SSID を削除してワイヤレスコントローラを再プロビジョニングする前に、対応するワイヤレス アプリケーション ポリシーを必ず削除してください。
- eWLC のワイヤレスアプリケーションは、学習された設定からプロビジョニングされた SSID ではサポートされません。
- Cisco DNA Center は、Cisco Catalyst IE 3300 高耐久性シリーズ スイッチおよび Cisco Catalyst IE 3400 Heavy Duty シリーズ スイッチに対する ACL ベースのアプリケーションポリシーのサポートを提供します。最大 8 つのポートベースのカスタムアプリケーションを展開できます。ただし、DSCP ベースのアプリケーションには制限はありません。

（注） Cisco DNA Center では、AireOS および eWLC プラットフォームの FlexConnect ローカルスイッチングモードはサポートされていません。

アプリケーション ポリシーの管理

ここでは、アプリケーション ポリシーの管理の方法に関する情報について説明します。

前提条件

アプリケーションポリシーを設定する場合は、次の要件を満たしていることを確認してください。

- Cisco DNA Center は、ほとんどの Cisco LAN、WAN、WLAN デバイスをサポートします。お使いのネットワーク内でデバイスとソフトウェアバージョンがサポートされているかどうかを確認するには、*Cisco DNA Center* のサポート対象デバイス を参照してください。
- ISR-G2、ASR 1000、ワイヤレス LAN コントローラなど、シスコのネットワーク デバイスに AVC（Application Visibility and Control）機能のライセンスがインストールされていることを確認します。詳細については、「*NBAR2 (Next Generation NBAR) Protocol Pack FAQ*」を参照してください。
- AVC サポートは、スイッチで自動 QoS が設定されていない場合にのみ、IOS XE バージョン 16.9 を実行しているスイッチで使用できます。AVC サポートを利用するには、自動 QoS 設定のスイッチを IOS XE バージョン 16.11 以降にアップグレードする必要があります。
- ポリシーが必要な WAN インターフェイスを Cisco DNA Center で特定するには、インターフェイス タイプ（WAN）および（必要に応じて）副回線レートとサービス プロバイダのサービス クラス モデルを指定する必要があります。詳細については、サービス プロバイダ プロファイルの WAN インターフェイスへの割り当て （85 ページ）を参照してください。

- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、デバイスのロールの変更（インベントリ）を参照してください。

アプリケーション ポリシーの作成

ここでは、アプリケーションポリシーの作成方法について説明します。

始める前に

- ビジネス目標を定義します。例えば、ネットワーク応答時間を最短化させたり、非ビジネスアプリケーションを特定して優先度を下げたりすることで、ユーザの生産性を向上させるようなものです。これらの目標に基づいて、どのビジネスとの関連性カテゴリがアプリケーションに分類されるかを決定します。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、デバイスのロールの変更（インベントリ）を参照してください。
- サイトへのデバイスの追加詳細については、「デバイスをサイトに追加する」を参照してください。
- SP向けのトラフィック用に対してこのポリシーをSPプロファイルで設定する場合は、SPプロファイルが設定されていることを確認してください。アプリケーションポリシーの作成後にSPプロファイルに戻り、SLA属性をカスタマイズしてSPプロファイルをWANインターフェイスに割り当てます。詳細については、サービス プロバイダ プロファイルの設定を参照してください。

ステップ1 Cisco DNA Center GUIで[Menu]アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ2 [Add Policy]をクリックします。

ステップ3 [アプリケーション ポリシー名（Application Policy Name）]フィールドに、ポリシーの名前を入力します。

ステップ4 [有線（Wired）]または[ワイヤレス（Wireless）]ラジオ ボタンのいずれかを選択します。

ステップ5 ワイヤレスネットワークの場合は、[SSID]ドロップダウンリストからプロビジョニングされたSSIDを選択します。

ステップ6 [サイトの範囲（Site Scope）]をクリックし、展開するポリシーの横にあるチェック ボックスをオンにします。

（注） 有線デバイスのポリシーでは、別のポリシーに割り当て済みのサイトは選択することができません。ワイヤレス デバイスのポリシーでは、同じSSIDで別のポリシーに割り当て済みのサイトを選択することができません。

ステップ 7 有線デバイスのポリシーでは、デバイスまたは特定のインターフェイスがポリシーで設定されないようにすることができます。

a) [サイトの範囲（Site Scope）] ペインで、興味のあるサイトの横にある ⚙ をクリックします。

選択した範囲内のデバイスのリストが表示されます。

b) 除外するデバイスを見つけ、関連する [ポリシーの除外（Policy Exclusions）] 列にあるトグル ボタンをクリックします。

c) 特定のインターフェイスを除外するには、[Exclude Interfaces] をクリックします。

d) [Applicable Interfaces] のリストから、除外するインターフェイスの横にあるトグルボタンをクリックします。

デフォルトでは、[Applicable Interfaces] のみが表示されます。すべてのインターフェイスを表示するには、[Show] ドロップダウンリストから [All] を選択します。

e) [< Back to Devices in *Site-Name*] をクリックします。

f) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 8 WAN デバイスでは、特定のインターフェイスを設定できます。

a) [Site Scope] ペインで、目的のサイトの横にある ⚙ をクリックします。

b) サイトのデバイスのリストで、目的のデバイスの横にある [SP Profile Settings] 列の [Configure] をクリックします。

（注） このオプションは、ルータの場合にのみ使用可能です。

c) [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。

d) [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- 物理インターフェイス：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
- トンネルインターフェイス：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。

（注） これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

e) [サービス プロバイダ プロファイル（Service Provider Profile）] 列で、[プロファイルの選択（Select Profile）] ドロップダウン リストから SP プロファイルを選択します。

f) （任意） 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

g) （任意） 追加の WAN インターフェイスを設定するには、[+] をクリックし、手順 c ～ f を繰り返します。

h) **[Save]** をクリックします。

i) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 9 [サイトの範囲（Site Scope）] ペインで、[OK] をクリックします。

ステップ 10 （任意） Cisco Validated Design（CVD）キューイング プロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

a) [キューイング プロファイル（Queuing Profiles）] をクリックします。
b) 左ペインのリストから、キューイング プロファイルを選択します。
c) [Select] をクリックします。

ステップ 11 （任意） このポリシーが SP 向けトラフィックである場合は、SP プロファイルの SLA 属性をカスタマイズします。

a) [SP プロファイル（SP Profile）] をクリックします。
b) SP プロファイルを選択します。
c) SLA 属性をカスタマイズします（[DSCP]、[SP 帯域幅（%）（SP Bandwidth %）]、および [キューイング帯域幅（%）（Queuing Bandwidth %）]）。

ステップ 12 （任意） ネットワークで使用されるアプリケーション セットのビジネスとの関連性を設定します。

Cisco DNA Center には、ビジネス関連性グループに事前設定されたアプリケーション セットが付属しています。あるビジネス関連性グループから別のグループにアプリケーションセットをドラッグアンドドロップして、この設定を維持したり、変更したりすることができます。

お気に入りとしてマークされたアプリケーションは、アプリケーションセットの上部に表示されます。お気に入りを変更するには、[Applications registry] に移動します。

ステップ 13 （任意） コンシューマを作成してアプリケーションに割り当てるか、アプリケーションを双方向としてマークすることにより、アプリケーションをカスタマイズします。

a) アプリケーション グループを展開します。
b) 目的のアプリケーションの横にある歯車アイコン ⚙ をクリックします。
c) [トラフィックの方向（Traffic Direction）] エリアで、[単方向（Unidirectional）] または [双方向（Bi-directional）] ラジオ ボタンを選択します。
d) 既存のコンシューマを選択するには、[コンシューマ（Consumer）] ドロップダウン リストから設定するコンシューマを選択します。新しいコンシューマを作成するには、[+ コンシューマの追加（+ Add Consumer）] をクリックして、[コンシューマ名（Consumer Name）]、[IP/サブネット（IP/Subnet）]、[プロトコル（Protocol）]、および [ポート/範囲（Port/Range）] を定義します。
e) [OK] をクリックします。

ステップ 14 ホスト トラッキングを設定します。[ホスト トラッキング（Host Tracking）] トグル ボタンをクリックして、ホスト トラッキングのオンとオフを切り替えます。

アプリケーションポリシーを展開する際に、Cisco DNA Center では、コラボレーション エンドポイント（テレプレゼンスユニットやシスコ電話など）が接続されているスイッチに、ACL のエントリを自動的に適用します。

ACE は、コラボレーション エンドポイントによって生成された音声およびビデオトラフィックを照合し、音声およびビデオトラフィックが正しくマークされるようにします。

ホストトラッキングがオンの場合、Cisco DNA Center はサイトの範囲内でコラボレーション エンドポイントの接続をトラッキングし、コラボレーション エンドポイントがネットワークに接続されるか、1 つ

のインターフェイスから別のインターフェイスに移動したときに、ACL エントリを自動的に再設定します。

ホストトラッキングが終了すると、Cisco DNA Center は、コラボレーション エンドポイントが新しいインターフェイスに移動または接続したときに、デバイスにポリシーを自動的に展開しません。代わりに、コラボレーションエンドポイントで正しく設定されるように、ACL のポリシーを再展開する必要があります。

ステップ 15 （任意） デバイスに送信される CLI コマンドをプレビューします。詳細については、「アプリケーション ポリシーのプレビュー （80 ページ）」を参照してください。

ステップ 16 （任意） ポリシーを展開するデバイスを事前にチェックします。詳細については、「アプリケーションポリシーの事前チェック （81 ページ）」を参照してください。

ステップ 17 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （65 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに展開するには、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー展開をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、ポリシーのスケジューリング （67 ページ）を参照してください。

  （注） アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシー情報の表示

作成および展開したアプリケーション ポリシーに関するさまざまな情報を表示できます。

始める前に

少なくとも 1 つの展開されたアプリケーション ポリシーがなければなりません。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを名前で並べ替えたり、名前、ステータス、キューイング プロファイルによってフィルタ処理したりします。

ステップ 3 ポリシーのリストと、それぞれに関する次の情報が表示されます。

- [Policy Name]：ポリシーの名前。

- [Version]：ポリシーの反復。ポリシーが展開されるか、または、ドラフトとして保存されるたびに、バージョンが 1 ずつ増分されます。たとえば、ポリシーを作成して展開すると、ポリシーはバージョン 1 になります。ポリシーを変更して、再度展開すると、ポリシーのバージョンはバージョン 2 に増分されます。詳細については、ポリシーのドラフト （65 ページ）およびポリシーのバージョン管理（67 ページ）を参照してください。
- [Policy Status]：ポリシーの状態。Cisco Catalyst 3850、Catalyst 4500、および Catalyst 9000 デバイスに適用されたポリシーがポートチャネルの更新（作成/変更/削除）によって影響を受ける場合は、アラートがポリシーステータスに表示されます。
- [Deployment Status]：最新の展開の状態（デバイスごと）。次の概要を示します。
  - 正常にプロビジョニングされたデバイス
  - プロビジョニングに失敗したデバイス
  - 展開が終了したためにプロビジョニングされなかったデバイス。

  最新の導入の状態をクリックすると、[ポリシーの展開（Policy Deployment）] ウィンドウが表示され、ポリシーが展開されたデバイスのフィルタ処理可能なリストが示されます。デバイスごとに、次の情報が表示されます。
  - デバイスの詳細（名前、サイト、タイプ、ロール、および IP アドレス）
  - 成功した導入のステータス。ステータスの横にある歯車のアイコンをクリックすると、[Effective Marking Policy] ウィンドウが開き、[Business Relevant] および [Business Irrelevant] アプリケーションと、それらが最終的に渡されるトラフィッククラスキューが表示されます。TCAM リソースまたは古いNBARプロトコルパックに限定されているデバイスの場合は、ポリシーに含まれるアプリケーションのサブセットのみをプロビジョニングでき、それらがビューで表示されます。
  - 障害ステータスには、障害の理由が示されます。
- [Scope]：ポリシーに割り当てられているサイト（デバイスではなく）の数。ワイヤレスデバイスのポリシーの場合は、ポリシーの適用先の SSID の名前が含まれます。
- [LAN Queuing Profile]：ポリシーに割り当てられている LAN キューイングプロファイルの名前。

アプリケーション ポリシーの編集

アプリケーション ポリシーを編集できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 対応するポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 必要に応じて、アプリケーション ポリシーを変更します。

ステップ 6 アプリケーションのビジネスとの関連性を変更するには、ビジネス関連、ビジネスと無関係、およびデフォルトグループの間でアプリケーションセットを移動します。

アプリケーションポリシーの設定については、アプリケーション ポリシーの作成 （71 ページ）を参照してください。

ステップ 7 キューイングプロファイルを更新するには、[Queuing Profiles] をクリックし、左ペインのリストからキューイングプロファイルを選択します。

ステップ 8 [Select] をクリックします。

ステップ 9 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （65 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。詳細については、ポリシーのスケジューリング （67 ページ）を参照してください。

  （注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーション ポリシーのドラフトの保存

ポリシーを作成、編集、または複製する際、ドラフトとして保存し、後で変更を続けることができます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを作成、編集、または複製します。

ステップ 3 [ドラフトの保存（Save Draft）] をクリックします。

詳細については、ポリシーのドラフト （65 ページ）を参照してください。

アプリケーション ポリシーの展開

新しいアプリケーションの追加や、アプリケーションをお気に入りとしてマークするなど、ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再展開する必要があります。

（注） IOS バージョン 16.x 以降を搭載した Cisco Catalyst 3850、Catalyst 3650、および Catalyst 9000 デバイスでは、ポリシーを展開する前に、自動 QoS 設定が自動的に削除されます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 導入するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 導入するポリシーの横のラジオ ボタンをクリックします。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[導入（Deploy）] を選択します。

a) ポリシーを再展開すると、ポリシーの範囲から削除されたデバイスに対して適切なアクションを実行するように求められます。次のいずれかの適切なアクションを選択します。

- デバイスからポリシーを削除する（推奨）
- ポリシーの範囲からデバイスを削除する
- ポリシーの範囲からデバイスを削除し、デバイスをブラウンフィールド設定に復元する

b) [Apply] をクリックします。

ステップ 5 ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行（RunNow）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

ポリシー導入のキャンセル

[導入（Deploy）] をクリックすると、Cisco DNA Center は、サイト範囲内のデバイスに関するポリシーの設定を開始します。間違いが見つかった場合は、ポリシーの展開をキャンセルできます。

ポリシー設定プロセスはバッチ処理として実行され、一度に40台のデバイスが設定されます。デバイスが 40 台以下の場合にポリシーの展開をキャンセルしても、デバイスの最初のバッチへの展開がすでに行われているため、デバイスが設定されている可能性があります。ただし、何百台ものデバイスがある場合は、必要に応じてポリシーの展開をキャンセルできます。

[中止（Abort）] をクリックすると、Cisco DNA Center によって設定がまだ開始されていないデバイスの設定プロセスがキャンセルされ、デバイスのステータスが [ポリシーの中止（Policy Aborted）] に変更されます。Cisco DNA Center では、完了している、または完了する予定の処理での導入はキャンセルされません。これらのデバイスでは、更新されたポリシー設定が維持され、ポリシー設定の状態（設定中、成功、または失敗）が反映されます。

ポリシー導入中に [中止（Abort）] をクリックしてポリシー設定プロセスをキャンセルします。

アプリケーション ポリシーの削除

不要になったアプリケーション ポリシーを削除できます。

ポリシーを削除すると、クラスマップ、ポリシーマップ、およびポリシーマップとワイヤレス ポリシー プロファイルの関連付けが削除されます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 削除するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 削除するポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。

ステップ 5 [Undeploy Policy] ウィンドウで、[Delete policy from devices] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 削除を確定する場合は、[OK] をクリックします。それ以外の場合は、[Cancel] をクリックします。

ステップ 7 削除を確認するメッセージが表示されたら、[OK] を再度クリックします。

[Application Policies] ページで、ポリシーの削除ステータスを確認できます。ステータスに [deletion failed] と表示された場合は、次の手順を実行します。

a) [Application Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。
b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを削除します。

アプリケーション ポリシーの複製

既存のアプリケーションポリシーに、新しいポリシーで必要な設定のほとんどが含まれている場合は、既存のポリシーの複製し、変更してから異なる範囲に展開することで時間を節約できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 複製するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 複製するポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[複製（Clone）] を選択します。

ステップ 5 必要に応じてアプリケーション ポリシーを設定します。アプリケーション ポリシーの設定については、アプリケーション ポリシーの作成 （71 ページ）を参照してください。

ステップ 6 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （65 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、ポリシーのスケジューリング （67 ページ）を参照してください。

  （注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーション ポリシーの復元

ポリシーを作成または変更してから、最初からやり直すことを決定した場合、Cisco DNA Center を使ってこれを設定する前に、デバイスにあった元の QoS 設定を復元することができます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。

ステップ 5 [Undeploy Policy] ウィンドウで、[Restore devices to original configurations] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

[Application Policies] ページで、ポリシーの復元ステータスを確認できます。ステータスに [restoration failed] と表示された場合は、次の手順を実行します。

a) [Application Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。

b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを復元します。

デフォルトの CVD アプリケーション ポリシーをリセット

CVD 設定は、アプリケーションのデフォルト設定です。ポリシーの作成または変更を行った後で最初からやり直す必要が生じた場合は、アプリケーションを CVD 設定にリセットすることができます。CVD 設定の詳細については、アプリケーション ポリシー （54 ページ）を参照してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

ステップ 7 次のいずれか 1 つのタスクを実行します。

- ポリシーのドラフトを保存するには、[ドラフトの保存（Save Draft）] をクリックします。
- ポリシーを展開するには、[展開（Deploy）] をクリックします。

アプリケーション ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用する CLI を生成して設定をプレビューできます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 アプリケーション ポリシーの作成 （71 ページ）またはアプリケーション ポリシーの編集 （75 ページ）の説明に従って、ポリシーを作成または編集します。

ステップ 3 ポリシーを展開する前に、[プレビュー（Preview）] をクリックします。

範囲内のデバイスのリストが表示されます。

ステップ 4 対象のデバイスの横にある [生成（Generate）] をクリックします。

Cisco DNA Center により、ポリシーの CLI が生成されます。

ステップ 5 [表示（View）] をクリックして CLI を表示するか、CLI をクリップボードにコピーします。

アプリケーション ポリシーの事前チェック

アプリケーションポリシーを展開する前に、サイト範囲内のデバイスがサポート対象であるかどうかをチェックできます。事前チェック プロセスには、デバイスのモデル、ラインカード、およびソフトウェア イメージの検証が含まれます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 アプリケーション ポリシーの作成 （71 ページ）またはアプリケーション ポリシーの編集 （75 ページ）の説明に従って、ポリシーを作成または編集します。

ステップ 3 [事前チェック（Pre-check）] をクリックします。

Cisco DNA Center は、デバイスをチェックして、問題があれば [事前チェック結果（Pre-Check Result）] 列に内容を報告します。[Errors] タブには、このポリシーをサポートしていないデバイスが表示されます。[Warnings] タブには、デバイスにこのポリシーを展開することを選択した場合に、サポートされていない制限や機能が表示されます。[Warnings] タブに一覧表示されているデバイスのポリシーを展開することもできます。問題を解決するには、Cisco DNA Center のサポート対象デバイスに記載されている仕様にデバイスを準拠させます。

アプリケーション ポリシー履歴の表示

アプリケーションポリシーのバージョン履歴を表示できます。バージョン履歴には、ポリシーのシリーズ番号（反復）と、バージョンが保存された日付と時刻が含まれています。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン リストから、[履歴（History）] を選択します。

ステップ 4 [ポリシー履歴（Policy History）] ダイアログボックスでは、次のことを実行できます。

- 現在のバージョンとバージョンを比較するには、関心のあるバージョンの横にある [差異（Difference）] をクリックします。
- ポリシーの前のバージョンにロールバックするには、ロールバック先となるバージョンの横にある [ロールバック（Rollback）] をクリックします。

ポリシーの以前のバージョンにロール バック

ポリシー設定を変更し、その後その設定が不適切だと判明した場合、またはネットワークで目的の効果が得られなかった場合、最大で 5 バージョン前のポリシーに戻すことができます。

始める前に

以前のポリシーバージョンにロールバックするには、少なくとも2つのポリシーバージョンを作成しておく必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウンリストから、[履歴の表示（Show History）] を選択します。

選択したポリシーの以前のバージョンは降順に表示され、最も新しいバージョン（最も大きい番号）が一覧の最上部に表示され、最も古いバージョン（最も小さい番号）が最下部に表示されます。

ステップ 4 （任意） 選択したバージョンと最新バージョンの間の差異を表示するには、[View] 列で [Difference] をクリックします。

ステップ 5 ロールバックする先のポリシー バージョンを決定した場合、そのポリシー バージョンに対して [Rollback] をクリックします。

（注） 選択したサイトの範囲がポリシー バージョン間で変更された場合、ロールバックは選択されている現在（最新）のサイトでは行われません。ポリシーのコンテンツのみがロールバックされます。

ステップ 6 [OK] をクリックして、ロールバック手順を確定します。

ロールバック先のバージョンが最新バージョンになります。

キューイング プロファイルの管理

次のセクションでは、キューイングプロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

キューイング プロファイルの作成

Cisco DNA Center では、デフォルトの CVD キューイング プロファイル（CVD_QUEUING_PROFILE）を提供します。このキューイングプロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[Application]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [Add Profile] をクリックします。

ステップ 3 [Profile Name] フィールドに、プロファイルの名前を入力します。

ステップ 4 スライダを使用して各トラフィック クラスに帯域幅を設定します。プラス記号（+）またはマイナス（-）記号をクリックするか、フィールドに特定の数値を入力します。

数値は、選択したアプリケーション クラスに確保されるインターフェイス帯域幅の合計に対しての割合を示します。帯域幅の合計は 100 なので、1 つのアプリケーション クラスに帯域幅を追加すると、別のアプリケーション クラスから帯域幅が差し引かれます。

開いた錠のアイコンは、そのアプリケーション クラスの帯域幅を編集できることを示します。閉じた錠のアイコンは、編集できないことを示します。

間違えた場合は、[シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックして CVD 設定に戻ることができます。

中央のグラフは、各アプリケーション クラスを設定している帯域幅の量の視覚化に役立ちます。

ステップ 5 （高度なユーザー向け）Cisco DNA Center が各トラフィック クラスで使用する DSCP コード ポイントをカスタマイズするには、[表示（Show）] ドロップダウン リストで、[DSCP値（DSCP Values）] を選択し、フィールドに特定の数値を入力して、各アプリケーション クラスの値を設定します。

SP のクラウド内で必要な DSCP コード ポイントをカスタマイズするには、SP のプロファイルを設定します。

ステップ 6 [Save] をクリックします。

キューイング プロファイルの編集または削除

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [キューイング プロファイル（Queuing Profile）] ペインで、編集または削除するキューイング プロファイルの横にあるラジオ ボタンをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- プロファイルを編集するには、プロファイル名を除くフィールドの値を変更し、[保存（Save）] をクリックします。フィールドの詳細については、キューイング プロファイルの作成 （82 ページ）を参照してください。
- プロファイルを削除するには、[削除（Delete）] をクリックします。

  アプリケーション ポリシーによって参照されている場合は、キューイング プロファイルを削除できません。

WAN インターフェイスのアプリケーション ポリシーの管理

次のセクションでは、WAN インターフェイスのアプリケーション プロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

サービス プロバイダ プロファイルの SLA 属性をカスタマイズ

自身のクラス モデルによって SP プロファイルに割り当てられたデフォルトの SLA 属性を使用しない場合は、要件に合わせて SP プロファイルの SLA 属性をカスタマイズすることができます。SP プロファイルのデフォルトの SLA 属性の詳細については、サービス プロバイダのプロファイル （59 ページ）を参照してください。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 変更するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [SPプロファイル（SP Profiles）] をクリックし、SP プロファイルを選択します。

ステップ 6 次のフィールドの情報を変更できます。

- [DSCP]：Differentiated Services Code Point（DSCP）値。有効値は 0 ～ 63 です。
  - Expedited Forwarding（EF）
  - クラスセレクタ（CS）：CS1、CS2、CS3、CS4、CS5、CS6
  - 相対的優先転送：AF11、AF21、AF41
  - [Default Forwarding (DF)]

  これらの DSCP 値の詳細については、マーキング、キューイング、ドロッピングの処理 （57 ページ）を参照してください。
- [SP Bandwidth %]：特定のサービスクラスに割り当てられた帯域幅の割合。
- [Queuing Bandwidth %]：各トラフィッククラスに割り当てられた帯域幅の割合。次のうちいずれかの変更を行うことができます。
  - キューイング帯域幅をカスタマイズするには、鍵アイコンをクリックして、帯域幅の設定をアンロックし、帯域幅の割合を調整します。
  - SP 帯域幅から自動的にキューイング帯域幅を計算するには、鍵アイコンをクリックしてキューイング帯域幅の設定をロックし、次に [OK] をクリックして確認します。デフォルトでは、Cisco DNA Center は、SP クラスのすべてのトラフィック クラスのキューイング帯域幅の合計がそのクラスの SP 帯域幅の割合と一致するように、キューイング帯域幅の割合を自動的に配信します。

ステップ 7 [OK] をクリックします。

サービス プロバイダ プロファイルの WAN インターフェイスへの割り当て

アプリケーション ポリシーがすでに作成済みで、SP プロファイルを WAN インターフェイスに割り当てる場合は、ポリシーを編集してこの設定を実行し、必要に応じてインターフェイスに Subline Rate の設定を含めます。

始める前に

ポリシーを作成していない場合は、ポリシーを作成し、同時に SP プロファイルを WAN インターフェイスに割り当てることができます。詳細については、「アプリケーション ポリシーの作成 （71 ページ）」を参照してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [Site Scope] ペインで、対象のサイトの横にある歯車アイコンをクリックします。

ステップ 6 対象のデバイスの [SPプロファイル設定（SP Profile Settings）] 列にある [設定（Configure）] をクリックします。

ステップ 7 [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。

ステップ 8 [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- **物理インターフェイス**：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
- **トンネルインターフェイス**：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。

  （注） これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

ステップ 9 [サービス プロバイダー プロファイル（Service Provider Profile）] 列で、[プロファイルの選択（Select Profile）] ドロップダウン フィールドをクリックし、SP プロファイルを選択します。

ステップ 10 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

ステップ 11 追加の WAN インターフェイスを設定するには [+] をクリックし、ステップ 7 ～ 10 を繰り返します。

ステップ 12 **[Save]** をクリックします。

ステップ 13 [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 14 [OK] をクリックします。

ステップ 15 [Deploy] をクリックします。

ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。

ステップ 16 次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオ ボタンをクリックし、[適用（Apply）] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

トラフィック コピー ポリシー

Cisco DNA Center を使用して、2 つのエンティティ間の IP トラフィック フローがモニターリングまたはトラブルシューティングのために指定された宛先にコピーされるように Encapsulated Remote Switched Port Analyzer（ERSPAN）を設定できます。

Cisco DNA Center を使用して ERSPAN を設定するには、コピーするトラフィック フローの送信元と宛先を定義するトラフィック コピー ポリシーを作成します。トラフィックのコピーを送信するデバイスおよびインターフェイスを指定するトラフィック コピー契約も定義できます。

（注） トラフィック コピー ポリシーにはスケーラブル グループまたは IP ネットワーク グループのいずれかを含めることができるため、このガイド全体を通して、グループという用語を使用する場合は他に指定がなければスケーラブル グループおよび IP ネットワーク グループの両方を指します。

送信元、宛先、およびトラフィックのコピー先

Cisco DNA Center トラフィックのモニターリングプロセスを簡素化します。物理ネットワーク トポロジを知っている必要はありません。必要なのは、トラフィック フローの送信元および宛先とコピーされたトラフィックの宛先となるトラフィック コピーの宛先を定義することだけです。

- [送信元（Source）] : モニターするトラフィックが通過する 1 つまたは複数のネットワーク デバイス インターフェイス。このインターフェイスは、エンドポイント デバイス、これらのデバイスの特定ユーザー、またはアプリケーションに接続することがあります。送信元グループを構成できるのは、イーサネット、ファストイーサネット、ギガビットイー

サネット、10 ギガビット イーサネット、またはポート チャネル インターフェイスのみです。

- [宛先（Destination）]：モニターするトラフィックが流れる IP サブネットです。IP サブネットはサーバー、リモート ピア、またはアプリケーションに接続することがあります。
- [トラフィックコピーの宛先（Traffic Copy Destination）]：ERSPAN データを受信、処理、および分析するデバイス上にあるレイヤ 2 またはレイヤ 3 の LAN インターフェイス。このデバイスは、通常、分析用にトラフィックのコピーを受信するパケット キャプチャ ツールまたはネットワーク分析ツールになります。

（注） 宛先では、スイッチ プローブ デバイスなどのネットワーク アナライザやその他のリモート モニターリング（RMON）プローブを使用してトラフィック分析を実行することを推奨します。

使用可能なインターフェイス タイプは、イーサネット、ファスト イーサネット、ギガビット イーサネット、または 10 ギガビット イーサネットのみです。宛先として設定されると、そのインターフェイスはコピーされたトラフィックのみを受信するために使用されます。このインターフェイスは今後その他のタイプのトラフィックを受信できなくなり、トラフィック コピー機能が必要とする以外のトラフィックを転送できません。トランク インターフェイスを宛先として設定できます。この設定により、インターフェイスはカプセル化されたトラフィックを送信できるようになります。

（注） 1 つのトラフィック コピー契約で使用できるトラフィック コピーの宛先は 1 つのみです。

トラフィック コピー ポリシーの注意事項と制限事項

トラフィック コピー ポリシー機能には次の制約事項があります。

- 最大 8 つのトラフィック コピー ポリシー、16 のコピー契約、および 16 のコピーの宛先を作成できます。
- 同じインターフェイスを複数のトラフィック コピーの宛先に使用することはできません。
- Cisco DNA Center は、トラフィック コピー ポリシーが変更され、ネットワークに展開されているポリシーとの整合性が失われていることを示すステータス メッセージを表示しません。ただし、トラフィック コピー ポリシーが展開された後に変更されたことが分かった場合は、そのポリシーを展開しなおすことができます。
- 管理インターフェイスを送信元グループまたはトラフィック コピーの宛先として設定することはできません。

トラフィック コピー ポリシー設定のワークフロー

始める前に

- モニター対象にする、トラフィック コピー ポリシーで使用されている送信元スケーラブル グループが、スイッチとそれらのインターフェイスに静的にマッピングされている必要があります。
- トラフィック コピー ポリシー宛先グループは、IP ネットワーク グループとして設定されている必要があります。詳細については、「IP ネットワーク グループの作成 （49 ページ）」を参照してください。

ステップ 1 トラフィック コピーの宛先を作成します。

これは、さらに分析するためにトラフィック フローがコピーされる、デバイス上のインターフェイスです。詳細については、トラフィック コピーの宛先の作成 （88 ページ）を参照してください。

ステップ 2 トラフィック コピーの契約を作成します。

契約はコピーの宛先を定義します。詳細については、トラフィック コピー契約の作成 （89 ページ）を参照してください。

ステップ 3 トラフィック コピー ポリシーを作成します。

ポリシーは、トラフィック フローの送信元と宛先、およびコピーされたトラフィックが送信される宛先を指定するトラフィック コピーの契約を定義します。詳細については、トラフィック コピー ポリシーの作成 （90 ページ）を参照してください。

トラフィック コピーの宛先の作成

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します[Policy] > [Traffic Copy] > [Traffic Copy Destination] の順に選択します。

ステップ 2 トラフィック コピーの宛先の名前と説明を入力します。

ステップ 3 デバイスと 1 つまたは複数のポートを選択します。

ステップ 4 [Save] をクリックします。

トラフィック コピーの宛先の編集または削除

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[Policy] > [Traffic Copy] > [Traffic Copy Destination] の順に選択します。

ステップ 2 編集または削除する宛先の横にあるチェックボックスをオンにします。

ステップ 3 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 宛先を削除するには、**[削除（Delete）]** をクリックします。

トラフィック コピー契約の作成

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[Policy] > [Traffic Copy] > [Traffic Copy Contract] の順に選択します。

ステップ 2 [Add]をクリックします。

ステップ 3 ダイアログボックスに、契約の名前と説明を入力します。

ステップ 4 **[コピー先（Copy Destination）]** ドロップダウン リストから、コピー先を選択します。

（注） コピー先は、1 つのトラフィック コピー契約に対し 1 つだけ指定できます。

選択可能なコピー先がない場合は、1 つ作成できます。詳細については、トラフィック コピーの宛先の作成 （88 ページ）を参照してください。

ステップ 5 [Save] をクリックします。

トラフィック コピー契約の編集または削除

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[Policy] > [Traffic Copy] > [Traffic Copy Contract] の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにします。

ステップ 3 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 契約を削除するには、[削除（Delete）] をクリックします。

トラフィック コピー ポリシーの作成

ステップ 1 [Policy] > [Traffic Copy] > [Traffic Copy Policies] の順に選択します。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

ステップ 4 [説明（Description）] フィールドにポリシーを表す単語またはフレーズを入力します。

ステップ 5 [契約（Contract）] フィールドで、[契約の追加（Add Contract）] をクリックします。

ステップ 6 使用する契約の隣にあるラジオ ボタンをクリックし、次に [保存（Save）] をクリックします。

ステップ 7 [使用可能なグループ（Available Groups）] エリアから、[送信元（Source）]エリアにグループをドラッグ アンド ドロップします。

ステップ 8 [使用可能なグループ（Available Groups）]エリアから、[宛先（Destination）]エリアにグループをドラッグ アンド ドロップします。

ステップ 9 [Save] をクリックします。

トラフィックコピーポリシーの編集または削除

ステップ 1 [Policy] > [Traffic Copy] > [Traffic Copy Policies] の順に選択します。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します

ステップ 2 編集または削除したいポリシーの横のチェック ボックスをオンにします。

ステップ 3 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- ポリシーを削除するには、**[削除（Delete）]** をクリックします。

仮想ネットワーク

仮想ネットワークは、独立したルーティングおよびスイッチング環境です。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。

仮想ネットワークに入れることができるのは、割り当てられたユーザー グループのみです。仮想ネットワーク内で、ユーザーとデバイスは、アクセス ポリシーによって明示的にブロックされていなければ相互に通信できます。異なる仮想ネットワークにまたがるユーザーは、相互に通信できません。ただし、例外ポリシーを作成して、一部のユーザーに異なる仮想ネットワークをまたぐ通信を許可することができます。

一般的な使用例はビルディング管理です。照明、冷暖房空調（HVAC）システム、セキュリティ システムなどのビルディング システムからユーザー コミュニティをセグメント化する必要があります。このケースでは、ユーザー コミュニティとビルディング システムを 2 つ以上の仮想ネットワークにセグメント化して、ビルディング システムの不正アクセスをブロックします。

仮想ネットワークは、複数のサイト ロケーションやネットワーク ドメイン（ワイヤレス、キャンパス、および WAN）にまたがる場合があります。

デフォルトでは、Cisco DNA Center には単一の仮想ネットワークがあり、すべてのユーザーおよびエンドポイントがこの仮想ネットワークに属しています。Cisco DNA Center が Cisco Identity Services Engine（ISE）と統合されると、デフォルトの仮想ネットワークに Cisco ISE のユーザー グループおよびエンドポイントが移入されます。

Cisco DNA Center では、仮想ネットワークの概念はワイヤレス、キャンパス、および WAN ネットワークで共通です。仮想ネットワークが作成されたら、ワイヤレス、有線、または WAN 導入が組み合わされているサイトと関連付けることができます。たとえば、ワイヤレス デバイスと有線デバイスが含まれるキャンパス ファブリックがサイトで展開されている場合、仮想ネットワークの作成プロセスによってキャンパス ファブリックでサービス セット識別子（SSID）と Virtual Routing and Forwarding（VRF）の作成がトリガーされます。また、サイトに WAN ファブリックも展開されている場合、VRF がキャンパスから WAN に同様に拡張します。

サイトの設計および初期設定時に、ワイヤレス デバイス、有線スイッチ、および WAN ルータをサイトに追加できます。Cisco DNA Center は、仮想ネットワークと関連付けられたポリシーがサイトに対して作成されたことを検出し、それらを異なるデバイスに適用します。

仮想ネットワークに関する注意事項と制限事項

仮想ネットワークには次の注意事項と制約事項があります。

- VRF はすべてのドメインで共通です。VRF の最大数は、ドメイン内の VRF が最も少ないデバイスに基づきます。

ゲストアクセス用の複数の仮想ネットワーク

ゲストアクセス用に複数の仮想ネットワークを作成できます。この機能を使用すると、企業のトラフィックが存在しない場所で、ゲストトラフィック用に異なる仮想ネットワークを使用できます。ワイヤレスゲスト SSID を異なる仮想ネットワークの IP プールに制限なしでマッピングできるようになりました。

仮想ネットワークの作成

仮想ネットワークを作成し、物理ネットワークを複数の論理ネットワークにセグメント化することができます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Virtual Network]** の順に選択します。

ステップ 2 [Create Virtual Network] をクリックします。

[Create Virtual Network] スライドインペインが表示されます。

ステップ 3 **[Name]** フィールドに、仮想ネットワークの名前を入力します。

ステップ 4 （オプション）[vManage VPN] ドロップダウンリストから、vManage VPN を選択します。

vManage VPN サービスを追加する場合は、事前に vManage 設定を構成しておく必要があります。詳細については、『Cisco DNA Center Administrator Guide』を参照してください。

ステップ 5 仮想ネットワークをゲストネットワークとして設定するには、[Guest Virtual Network] チェックボックスをオンにします。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [Scalable Groups] 列で、[Add] をクリックしてスケーラブルグループを追加します。

[Add Scalable Group Associations] スライドインペインが表示されます。

ステップ 8 仮想ネットワークに追加するスケーラブルグループの横にあるチェックボックスをオンにし、[Save] をクリックします。

仮想ネットワークの編集または削除

仮想ネットワークから別の仮想ネットワークにスケーラブルグループを移動すると、スケーラブルグループのマッピングが変更されます。この変更によって、グループ内のユーザーまたはデバイスに影響が及ぶ可能性があることに注意してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Policy]** > **[Virtual Network]** の順に選択します。

ステップ 2 仮想ネットワークを編集するには、次のいずれかを実行します。

- 仮想ネットワークの名前をクリックします。
- 仮想ネットワークを選択し、[Actions] > [Edit] の順にクリックします。

[View Virtual Network] スライドインペインが表示されます。

フィールド	説明
名前（Name）	これは読み取り専用のフィールドです。仮想ネットワークの名前は編集できません。
Guest Virtual Network	ゲストネットワークとして仮想ネットワークを設定するには、このチェックボックスをオンにします。

フィールド	説明
スケーラブルグループ	スケーラブルグループを追加するには、[Scalable Groups] 列で [Add] をクリックします。[Add Scalable Group Associations] スライドインペインが表示されます。追加するスケーラブルグループの横にあるチェックボックスをオンにし、[Save] をクリックします。 仮想ネットワークに現在追加されているスケーラブルグループを編集または削除するには、次の手順を実行します。 **1.** [Scalable Groups] 列に表示されているリンクをクリックします。 [View Scalable Group Associations] スライドインペインが表示されます。 **2.** [Edit] をクリックします。 次のタブが表示されます。 • [All]：使用可能なすべてのスケーラブルグループが表示されます。仮想ネットワークに現在追加されているスケーラブルグループは青色で強調表示されます。 • [Associated Groups]：仮想ネットワークに現在追加されているスケーラブルグループが表示されます。 • [Other]：仮想ネットワークに関連付けられていないスケーラブルグループが表示されます。 **3.** 必要な変更を行って、[Save] をクリックします。

ステップ 3 仮想ネットワークを削除するには、削除する仮想ネットワークを選択し、[Actions] > [Delete] の順にクリックします。

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