

グループベースのアクセス コントロール ポリシーおよび分析の設定

- グループベースのアクセスコントロール （1 ページ）
- シスコのグループベースポリシー分析 （19 ページ）

グループベースのアクセスコントロール

Catalyst Center は、次の 2 つの方法で Software-Defined Access（SD-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。
- セキュリティグループは、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セキュリティグループを管理し、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。

Catalyst 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、*Catalyst Center* 管理者ガイド [英語] を参照してください。

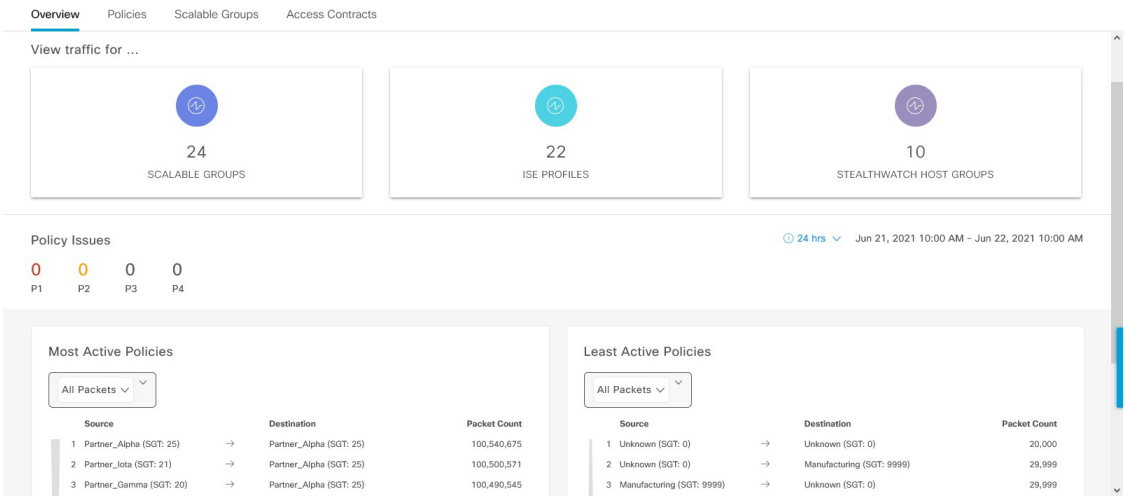
Cisco ISE 向け Catalyst Center の設定の詳細については、*Catalyst Center* 設置ガイド [英語] を参照してください。

Cisco ISE for Catalyst 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。

グループベースのアクセス コントロール ポリシー ダッシュボード

グループベースのアクセスコントロールポリシーダッシュボードでは、ネットワークアクティビティ、ポリシー関連の問題、およびトラフィックトレンドの概要が提供されます。このダッシュボードを表示するには、メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。

図 *1*: グループベースのアクセス コントロール ポリシー ダッシュボード



このダッシュボードでは、次の詳細を表示できます。

- [View Traffic]：セキュリティグループ、Cisco ISE プロファイル、および Stealthwatch ホストグループのトラフィックを表示できます。このデータを表示するには、グループベースポリシー分析パッケージをインストールする必要があります。グループベースポリシー分析で提供される分析情報により、新しいアクセスコントロールの導入による影響を評価するために、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、その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することができます。シスコのグルー

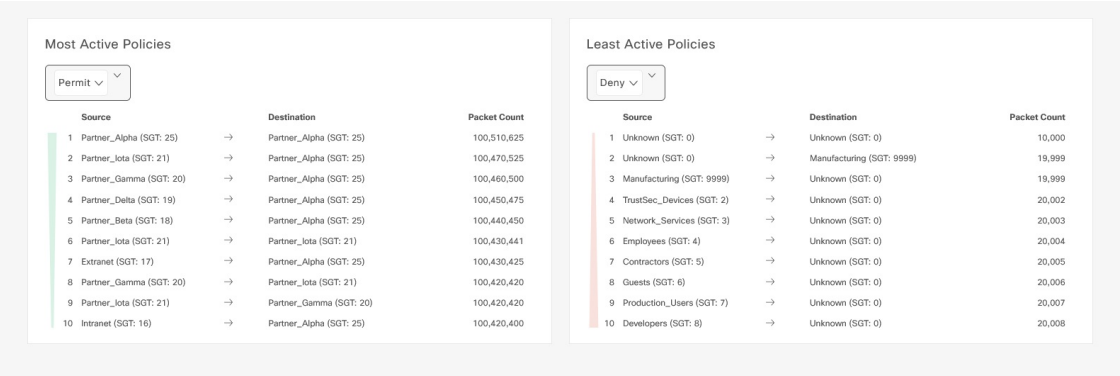
プベースポリシー分析では、ネットワーク上のアセットのグループとそれらの通信に関する情報が集約されます。詳細については、シスコのグループベースポリシー分析（19ページ）を参照してください。

- [View Policy-Related Issues]：ポリシー関連の問題の数が表示されます。数をクリックすると詳細情報が表示されます。新しいブラウザタブで [Assurance Issues] ダッシュボードが開きます。ここで、詳細情報を確認できます。

（注） このポリシー関連の問題のビューは、現在選択されている期間のものとなります。必要に応じて、時間セレクタを使用して時間枠を調整します。

- [View Most Active and Least Active Policies]：最もアクティブなポリシーと最もアクティブでないポリシーの詳細情報が提供されます。デフォルトでは、このビューは、各ポリシー（各送信元/宛先グループペア）に関してネットワークで確認されたパケットの総数に基づいています。ドロップダウンリストを使用して、許可されたパケットまたはドロップされたパケットのみを選択することができます。ドロップされたパケットのオプションを使用すると、ポリシーベースのドロップが最もアクティブに実行されているポリシーを確認することができます。

図 *2:* 最もアクティブなポリシーのダッシュレットと最もアクティブでないポリシーのダッシュレット



（注） このポリシーアクティビティのビューは、現在選択されている期間のものとなります。必要に応じて、時間セレクタを使用して時間枠を調整します。

グループベースのアクセス コントロール ポリシー

アクセス コントロール ポリシーでは、送信元セキュリティグループから宛先セキュリティ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。

- [Security Group]：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。セキュリティグループは、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、セキュリティ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。

- [Contract]：アクセス契約は、送信元と宛先のセキュリティ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。

  セキュリティ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、前に作成したセキュリティ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セキュリティ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、請負業者送信元セキュリティ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。財務サーバー宛先セキュリティ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。

  送信元と宛先のセキュリティグループの組み合わせに契約が指定されていない場合に使用され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] ウィンドウの右上隅にある [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、請負業者送信元セキュリティ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。財務サーバー宛先セキュリティ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、次の点を考慮してください。

- 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 Catalyst Center に追加され、サイトに割り当てられると、TrustSec 適用アクションが呼び出されます。
- Software-Defined Access（SD-Access）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>
```

- アップグレード後、[プロビジョニング（Provision）] > [ネットワークデバイス（Network Devices）] > [インベントリ（Inventory）] ウィンドウに次のメッセージが表示されます。

  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。

マトリックスビュー

[Group-Based Access Control] ウィンドウの右上隅にある [Grid] アイコンをクリックして、[Matrix] ビューを起動します。[Matrix] ビューは中核となるポリシービューであり、すべてのセキュリティグループのすべてのポリシー（明示的とデフォルトの両方）の概要を提供します。[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セキュリティ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セキュリティグループがリストされます。

特定の送信元セキュリティグループと宛先セキュリティ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。色は、次のとおり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 [許可（Permit）]、[拒否（Deny）]、[カスタム（Custom）]、または [デフォルト（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。

[Matrix] ビューでは、セルを選択すると、そのセルと対応する行（送信元セキュリティグループ）と列（宛先セキュリティグループ）が強調表示されます。選択したセルの座標（送信元および接続先セキュリティグループ）がマトリックス コンテンツ エリアの近くに表示されます。

セルをクリックして、そのセルの [Create Policy] または [Edit Policy] スライドインペインを開きます。[Create Policy] スライドインペイン には、送信元と宛先のセキュリティ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。そのセルのポリシーのステータスとアクセス契約の更新のみ実行できます。

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から [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セキュリティ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から、[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セキュリティグループが表示されます。

カーソルをマトリックスコンテンツ領域でドラッグするか、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。カーソルをこの領域でドラッグして、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。

[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します。関心のあるポリシーのみに焦点を当てるフィルタを作成できます。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。

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. 特定した分類のセキュリティ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。

セキュリティグループの作成

始める前に

こ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。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Security Groups]** の順に選択します。

ステップ 2 [セキュリティグループの作成（Create Security Group）] をクリックします。

ステップ 3 [Create Security Group] スライドインペインで、セキュリティグループの名前と説明（任意）を入力します。

（注） [名前（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 (_)

セキュリティグループ名は英字で開始する必要があります。

Catalyst 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セキュリティ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 [Virtual Networks] ドロップダウンリストから、このセキュリティグループに関連付ける仮想ネットワークを選択します。デフォルトでは、デフォルトの仮想ネットワークが選択されています。

（注） Catalyst Center 2.3.3 以降が Cisco ISE 3.2 以降と統合されている場合、セキュリティグループは仮想ネットワークに関連付けられず、これらのリリースでは [仮想ネットワーク（Virtual Networks）] フィールドは表示されません。ただし、Cisco ISE 3.1 以前を使用している場合は、セキュリティグループと仮想ネットワークの関連付けの詳細が表示されます。

ステップ 5 セキュリティグループを 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 セキュリティグループを今すぐ作成するか、後でスケジュールするかを選択します。

[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要が

あります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Catalyst Center の統合方法の詳細については、『*Cisco Catalyst Center ITSM Integration Guide*』を参照してください。

[Security Groups] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を確認できます。**[Activities] [Tasks]** でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

（注） 名前が「ANY」またはタグ値が 0xFFFF/65535 のセキュリティグループは作成できません。セキュリティグループ ANY/65535 は、Catalyst Center デフォルトポリシーに使用される予約済みの内部セキュリティグループです。

セキュリティグループの編集

始める前に

こ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。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Security Groups]** の順に選択します。

ステップ 2 [Security Groups] ウィンドウで、編集するセキュリティグループの横にあるチェックボックスをオンにし、[Edit] をクリックします。

ステップ 3 [Edit Security Group] スライドインペインで、必要な変更を加えた後、次の操作を実行します。

- 変更をすぐに保存するには、[Save Now] をクリックします。
- 特定の時間に更新をスケジュールするには、[Schedule Later] をクリックします。[Scheduler] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。

セキュリティグループを更新する場合は、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。[Deploy Now] をクリックして変更をすぐに展開するか、[Deploy Later] をクリックして変更を後で展開します。

セキュリティグループの削除

始める前に

こ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。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Security Groups]** の順に選択します。

ステップ 2 削除するセキュリティ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 次のオプションのいずれかを選択します。

- セキュリティグループをすぐに削除するには、[Delete Now] をクリックします。
- 後でセキュリティグループを削除するには、[Delete Later] をクリックします。[Schedule Delete] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。

（注） セキュリティグループの [Policies] 列のリンクをクリックすると、そのセキュリティグループとそのグループが属するポリシーを使用するアクセスコントロールルールが表示されます。セキュリティグループがいずれかのアクセスポリシーで使用されている場合、そのセキュリティグループは削除できません。

Catalyst Center と Cisco ISE 間のセキュリティグループの同期

Catalyst Center 内のセキュリティグループを Cisco ISE と同期しているときは、次のように動作します。

- セキュリティグループが Catalyst 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。
- セキュリティグループが Cisco ISE に存在し、Catalyst Center に存在しない場合は、Catalyst Center に作成されます。
- セキュリティグループ名が Catalyst Center と Cisco ISE の両方で同じで、説明と ACI データが異なっている場合、Catalyst Center は Cisco ISE で指定されたデータを使用して更新されます。
- Catalyst Center と Cisco ISE でセキュリティグループ名が同じで、タグ値が異なっている場合、Cisco ISE で指定されたタグ値を持つ新しいセキュリティグループが Catalyst Center に

作成されます。Catalyst Center にすでにあるセキュリティグループの名前は、サフィックス **_DNAC** で更新されます。

- タグの値が同じでセキュリティグループ名が異なる場合、Catalyst Center のセキュリティグループ名が Cisco ISE で指定された名前で更新されます。

Cisco ISE との同期が完了していない場合は、セキュリティ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セキュリティ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。これらのセキュリティグループは、[Created In] 列の値が **ACI** となって [Security Groups] ウィンドウに表示されます。ACI から学習したセキュリティグループは編集も削除もできませんが、ポリシーで使用することはできます。

[Associated Contracts] 列には、ACI から学習したセキュリティグループに関連付けられている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、対応するセキュリティグループ設定が Cisco ISE で更新されます。Cisco ISE でセキュリティグループが作成されると、新しい EEPG が ACI に作成されます。

アクセス契約の作成

アクセス契約は、送信元と宛先のセキュリティ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。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。

始める前に

こ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。

手順

ステップ 1 メインメニューから次を選択します。**[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、必要な詳細を入力します。

[Modeled Access Contract] チェックボックスはデフォルトで有効になっています。これにより、Catalyst Center が基盤となるセキュリティグループ ACL（SGACL）の有効なコマンドを生成します。このオプションを有効にすると、アクセス契約は、基盤となるコマンドラインシンタックスを知らなくても作成および編集できるモデルに基づくようになります。

SGACL コマンドラインを直接入力し、アクセス契約をテキストとして保存する場合は、[Modeled Access Contract] チェックボックスをオフにします。 入力したコマンドラインのテキストに対してシンタックス チェックは行われません。コマンドシンタックスが有効であることを確認する必要があります。



（注）
- このオプションは、アクセス契約の作成時にのみ有効または無効にできます。既存のアクセス契約では、このオプションを更新できません。
- SGACL コマンドが高度なものは、Cisco ネットワーク デバイスでサポートされていない場合もあります。

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。
- [Application] ドロップダウンリストから、アクションを適用するアプリケーションを選択します。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 アクセス契約を今作成するか、後でスケジュールするかを選択します。

[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Catalyst Center の統合方法の詳細については、『Cisco Catalyst Center ITSM Integration Guide』を参照してください。

[Access Contract] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を表示できます。[Activities] > [Tasks] でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

アクセス契約の編集

始める前に

こ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。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Access Contracts] ウィンドウで、編集するアクセス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 [Actions] > [Edit] の順に選択します。

ステップ 4 [Edit Access Contract] ウィンドウで、必要な変更を行った後、アクセス契約を今すぐ更新するか、後で更新するようスケジュールするかを選択します。

[Filter] オプションを使用して、契約を検索できます。

既存のアクセス契約を複製し、必要な詳細情報を編集して新しいアクセス契約を作成できます。アクセス契約を複製すると、既存のアクセス契約に含まれるすべての情報がコピーされ、コピーされた契約は、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。[Save Now] をクリックして複製契約をすぐに作成するか、[Schedule Later] をクリックして複製契約を後で作成します。

セキュリティグループ、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、Catalyst 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。[Deploy Now] をクリックして変更をすぐに展開するか、[Deploy Later] をクリックして変更を後で展開します。

Cisco ISE は、Catalyst 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。

アクセス契約の削除

始める前に

こ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。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Access Contracts] ウィンドウで、削除するアクセス契約の横にあるチェックボックスをオンにして、アクセス契約を今すぐ削除するか、後で削除するようスケジュールするかを選択します。

[Access Contracts] ウィンドウではサンプル契約を表示できます。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。

アクセス契約を使用するポリシーを表示するには、そのアクセス契約の [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。

Catalyst Center と Cisco ISE 間のアクセス契約の同期

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

- 契約が Catalyst 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、Catalyst Center に存在しない場合は、Catalyst Center に作成されます。
- 契約名が Catalyst 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、Catalyst 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、Catalyst 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、Catalyst Center ではその解析やシンタックスチェックは行われません。Catalyst 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 Catalyst Center のデフォルトポリシーとして移行されます。

Cisco ISE との同期が完了していない場合、アクセス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 から学習したアクセス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から学習したセキュリティ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 から学習したセキュリティグループを接続先グループとして選択すると、関連するアクセス契約が [Preferred Contracts] タブに表示されます。[All Contracts] タブですべてのアクセス契約を確認できます。

グループベースのアクセス コントロール ポリシーの作成

セキュリティ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、前に作成したセキュリティ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セキュリティ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」送信元セキュリティ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」宛先セキュリティ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。

手順

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) 選択する送信元セキュリティ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。

必要なセキュリティグループが存在しない場合は、[Create Security Group] をクリックして新しいセキュリティグループを作成します。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

b) [Next] をクリックします。

c) 選択した送信元セキュリティグループにマッピングする宛先セキュリティグループを選択します。

必要に応じて、セキュリティグループの詳細を表示したり、セキュリティグループを編集したりできます。



（注） 送信元と宛先の間にポリシーがすでに存在する場合、セキュリティ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。必要に応じて、契約の詳細を表示および編集できます。

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。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。



（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、選択したセキュリティ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) ポリシーを今すぐ作成するか、後でスケジュールするかを選択します。

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) 選択する宛先セキュリティ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。

必要なセキュリティグループが存在しない場合は、[Create Security Group] をクリックして新しいセキュリティグループを作成します。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

b) [Next] をクリックします。

c) 選択した宛先セキュリティグループにマッピングする送信元セキュリティグループを選択します。

必要に応じて、セキュリティグループの詳細を表示したり、セキュリティグループを編集したりできます。



（注） 送信元と宛先の間にポリシーがすでに存在する場合、セキュリティ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。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

（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、選択したセキュリティ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) ポリシーを今すぐ作成するか、後でスケジュールするかを選択します。

[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Catalyst Center の統合方法の詳細については、『Cisco Catalyst Center ITSM Integration Guide』を参照してください。

[Policies] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を表示できます。[Activities] > [Tasks] でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

トラフィックフローに基づくグループベースのアクセスコントロールポリシーの更新

手順

ステップ 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 ポリシーを更新するセルをクリックします。

ステップ 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。

ステップ 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します。

[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。

ステップ 4 必要な変更を行った後、次のオプションのいずれかを選択します。

- **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。**

Catalyst Center と Cisco ISE の間のポリシーの同期

Catalyst 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 Catalyst 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、Catalyst Center に存在しない場合は、Catalyst Center に作成されます。
- Cisco ISE でポリシー契約が異なる場合、 Catalyst 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）。Catalyst 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、Catalyst 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

シスコのグループベースポリシー分析について

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

購入できる Catalyst Center のライセンスの種類は次のとおりです。

- Essentials
- Advantage
- Premier

Advantage と Premier ライセンスには、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

グループベースポリシー分析のインストール

シスコのグループベースポリシー分析は Catalyst 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。

グループベースポリシー分析をインストールするには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Software Management]** の順に選択します。

ステップ 2 [Available Applications for 2.3.xx-xxxxx] エリアまで下にスクロールし、[Group-Based Policy Analytics] を選択します。

ステップ 3 [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、Catalyst 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。

（注） 次の表に、スタンドアロン展開のパフォーマンスメトリックを示します。これらの値は、クラスタ内のノードの数とインストールされているパッケージの数によって異なる場合があります。

表 *1*: 評価指標

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 13,000
クライアント（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

メトリック	44 コア、3 ノード	56 コア	112 コア
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	シリーズ	Catalyst Center UI の [ネットワーク設定（Network Settings）] の [テレメトリ（Telemetry）] セクションで設定可能な NetFlow（Flexible NetFlow または Application Visibility and Control ベースの NetFlow）	Catalyst Center UI の CLI テンプレートツールを使用して設定可能な NetFlow（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	シリーズ	**Catalyst Center UI** の [ネットワーク設定（**Network Settings**）] の [テレメトリ（**Telemetry**）] セクションで設定可能な **NetFlow**（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Catalyst Center UI** の **CLI** テンプレート ツールを使用して設定可能な **NetFlow**（**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	はい	該当なし	対応
	Cisco Catalyst 3560 シリーズ	非対応	はい	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
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

Catalyst Center は、Cisco ISE 2.4 パッチ 7 以降、Cisco ISE 2.6 パッチ 1 以降、Cisco ISE 2.7 以降をサポートしています。

Cisco StealthWatch

Catalyst Center は、Cisco Stealthwatch 7.x 以降をサポートしています。

コネクタについて

Cisco グループベースポリシー分析は、コネクタとも呼ばれるさまざまなソースからテレメトリを収集します。シスコのグループベースポリシー分析の初期設定 （24 ページ） ワークフローに従うか、**[Policy]** > **[Group-Based Access Control]** > **[Analytics]** > **[Configurations]** > **[Analytics Settings]** の順に選択して、コネクタを設定できます。

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。Cisco ISE と Cisco Stealthwatch はグループデータコネクタです。

- **Cisco ISE**

  Cisco ISE は次世代の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 プラットフォームであり、企業がコンプライアンスを適用し、インフラストラクチャのセキュリティを強化し、サービス運用を合理化できるようにします。 Cisco ISE は、仮想マシン、物理マシン、または両マシンの組み合わせにインストールされます。 Cisco ISE は、セッションディレクトリ、セキュリティグループ、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 Cisco Platform Exchange Grid（pxGrid）サービスを使用します。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、Session Directory 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。セキュリティ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、セキュリティグループタグ（SGT）と呼ばれることもあり、SGT に応じてネットワークデバイスによるトラフィックのフィルタ処理を可能にすることで、Cisco ISE がアクセス コントロール ポリシーを適用できるようにします。

  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に関する情報を収集します。情報には、デバイスのタイプ、OS、OS 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、Cisco ISE の SGT 定義とプロファイルをシスコのグループベースポリシー分析に提供します。

- **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、Catalyst 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。Catalyst 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ポリシー分析の初期設定

このワークフローでは、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 Cisco ISE、Cisco Stealthwatch、NetFlow などの特定のソースから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

Catalyst 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。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。[確実なポリシーの作成（Create policies with more confidence）] ウィンドウが表示されます。

ステップ 2 [Get Started] をクリックします。
[データコネクタの設定（Configure your data connectors）] ウィンドウが表示されます。

ステップ 3 [Let's Do it] をクリックします。

[グループデータコネクタの設定（Configure Group Data Connectors）] ウィンドウが表示されます。

（注） 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、次のエラーメッセージが表示されます。

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、Catalyst 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

ステップ 5 [Settings] ウィンドウを閉じます。[グループデータコネクタの設定（Configure Group Data connectors）] ウィンドウで、正常に設定されたコネクタの [設定（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。
[通信コネクタの設定（Configure Communication Connectors）] ウィンドウが表示されます。

ステップ 7 次のいずれかのオプションを使用して、通信コネクタ（NetFlow）を設定します。

- Catalyst Center のデバイスインターフェイスで NetFlow を手動でプロビジョニングします。
- [CLI Templates] をクリックし、Catalyst Center の [CLI Templates] ツールを使用して NetFlow を設定します。
- [Telemetry in Network Settings] をクリックし、ネットワーク設定のテレメトリのセクションで NetFlow を設定します。

ステップ 8 [Next] をクリックします。
[Summary] ウィンドウにコネクタの設定の詳細情報が表示されます。

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

このセクションは、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

[概要（Overview）] ウィンドウの [セキュリティグループ（Security Groups）] ボックスに表示されている数をクリックすると、**[セキュリティグループの詳細（Explore Security Groups）]** ウィンドウが表示されます。このウィンドウでは、セキュリティグループのグループ間通信すべて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。

（注） これは、過去 14 日間に設定された [概要（Overview）] ウィンドウの時間範囲とは異なります。チャートには、特定の期間に一意のフロー数が多い送信元セキュリティグループなど、上位 25 の送信元セキュリティグループとその対応するやり取りが表示されます。

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。

テーブルビューで、特定の行の [See destinations] リンクをクリックすると、選択した送信元セキュリティグループに対応するすべての宛先セキュリティグループが表示されたウィンドウが開き、各宛先セキュリティグループの一意のフロー数が表示されます。

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。

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。

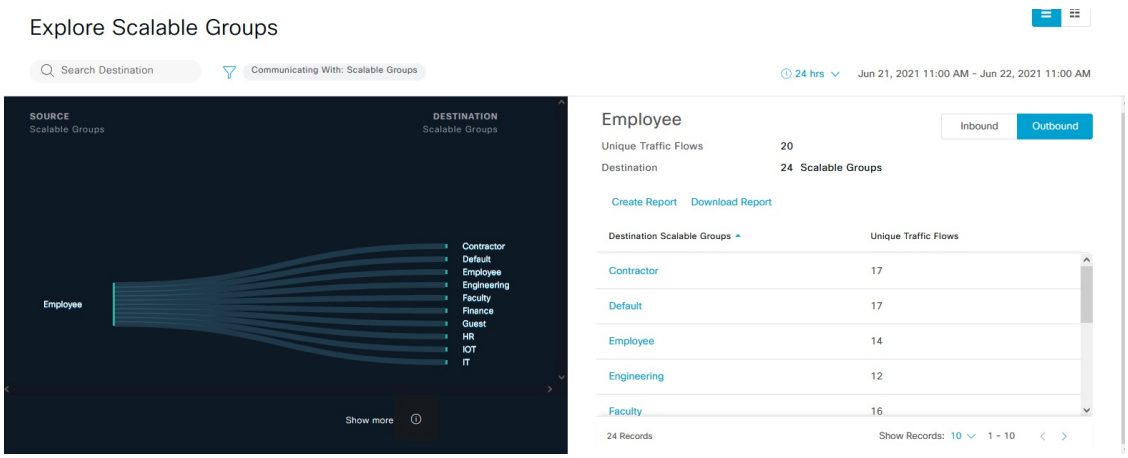
[概要（Overview）] ウィンドウの [ISEプロファイル（ISE Profiles）] ボックスに表示されている数をクリックすると、**[ISEプロファイルの詳細（Explore ISE Profiles）]** ウィンドウが表示されます。このウィンドウでは、送信元がISEプロファイルで宛先がセキュリティグループであるすべての通信の概要を確認できます。グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをセキュリティグループにする必要があります。

[概要（Overview）] ウィンドウの [Stealthwatchホストグループ（Stealthwatch Host Groups）] ボックスに表示されている数をクリックすると、**[Stealthwatchホストグループの詳細（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セキュリティグループであるすべての通信の概要を確認できます。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セキュリティグループにする必要があります。

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

このウィンドウには、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が表示されます。送信元と宛先の少なくとも一方がセキュリティ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。



 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。

[Outbound] をクリックすると、選択したセキュリティ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、このセキュリティ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。

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。

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。

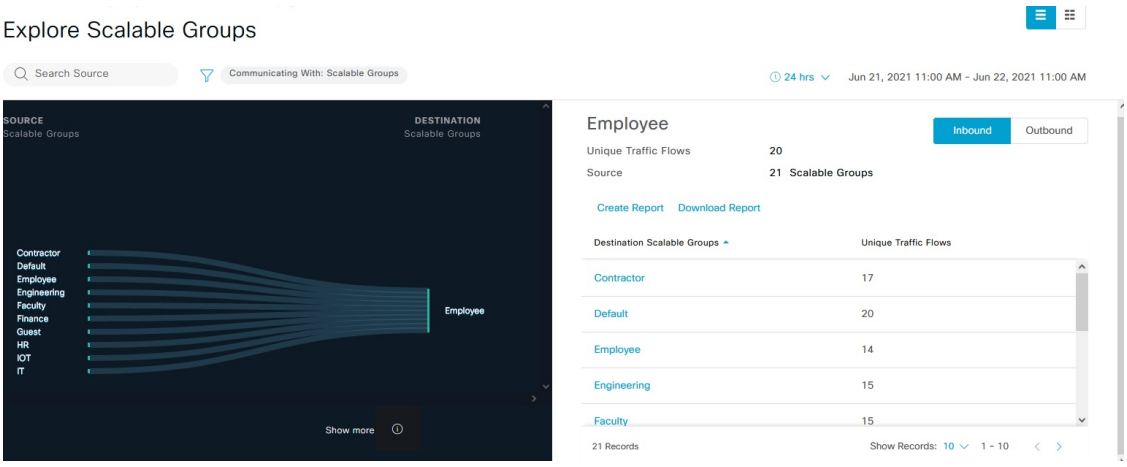
リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、**単一のグループから単一のグループ**のウィンドウに切り替わります。

[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。

単一のグループから複数のグループ：インバウンド

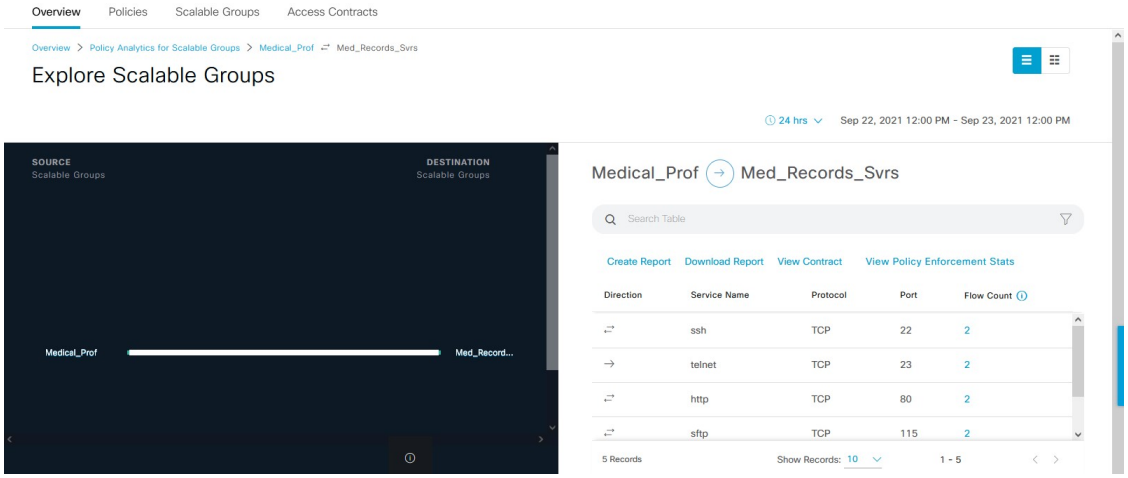
[Inbound] をクリックすると、選択したセキュリティグループを宛先としていずれかのグループから開始されたすべての接続が表示されます。



単一のグループから単一のグループ

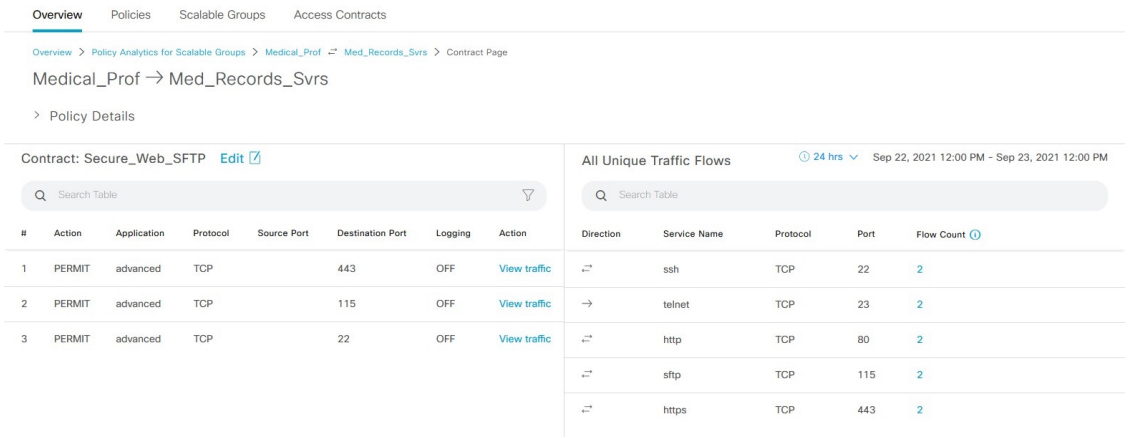
このウィンドウには、1 つの送信元グループと 1 つの宛先グループの間のアクティビティが表示されます。送信元グループと宛先グループの少なくとも一方がセキュリティグループである

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。

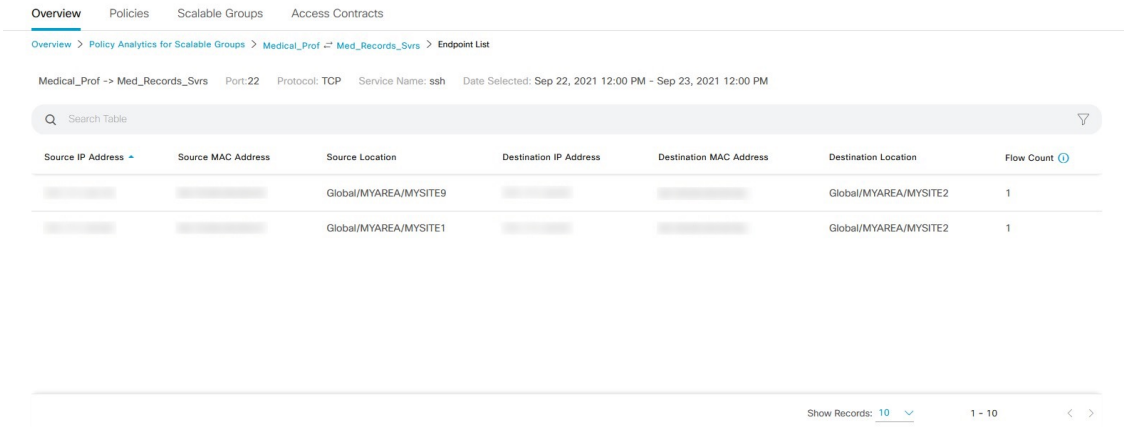


送信元グループと宛先グループの間に表示されている方向矢印をクリックすると、このビューの送信元グループと宛先グループが入れ替わります。

[View Contract] をクリックして、トラフィックフローと、この送信元と宛先グループのペアに有効なアクセス契約のルールを 1 対 1 で比較します。

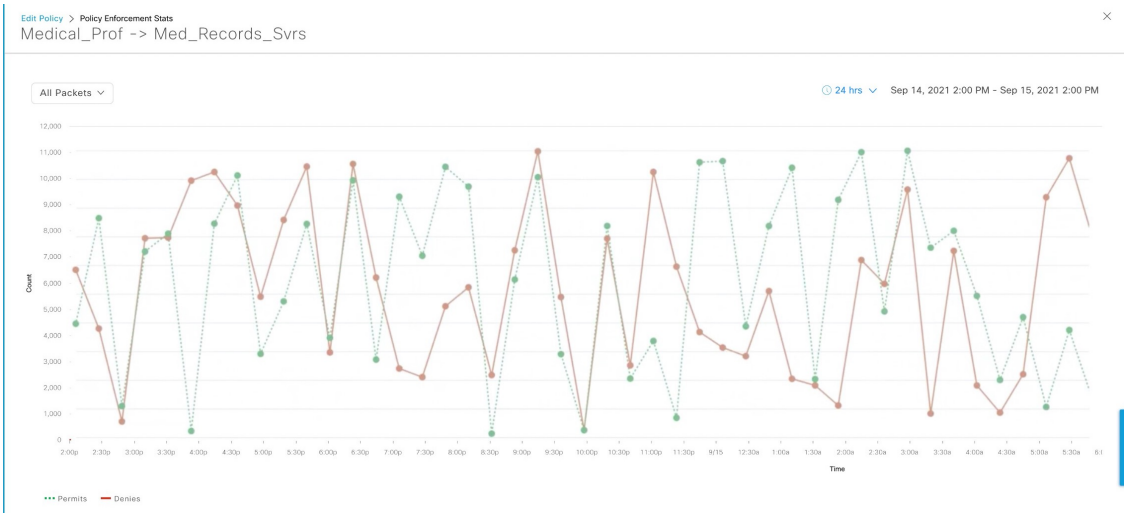


[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。右側のペインで、フローの方向、サービス名、フロー数、ポート、およびプロトコルの詳細を表示できます。[Flow Count] 列には、選択した期間に特定のサービス、ポート、およびプロトコルの組み合わせで検出されたフローの数が表示されます。フロー数のリンクをクリックして、各エンドポイントのフローの詳細を表示できます。



（注） フロー数に基づいて [トラフィックフロー（Traffic Flows）] テーブルを並べ替えると、1000 レコードのみが表示されます。

[View Policy Enforcement Stats] をクリックして、任意の送信元および宛先グループペアの許可カウントと拒否カウントの時系列グラフを表示します。これにより、ポリシーごとの適用統計情報が可視化されます。[All Packets] ドロップダウンリストを使用して、許可されたパケットまたはドロップされたパケットのみを選択することができます。グラフデータポイントは、15 分のデータ収集期間ごとに表示されます。データポイントにカーソルを合わせると、許可と拒否の数が表示されます。データポイントまたは期間をクリックして、選択した期間の契約とトラフィックフローの詳細を表示できます。



（注） フローデータの集計は 60 分ごとに実行されるため、選択した期間は、選択したデータポイントに対応する 15 分間隔を含む時間です。

ポリシーの作成または編集中に、[Policy Details] スライドインペインから [Traffic Flows] テーブルにアクセスすることもできます。

 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。

[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。

アクセス契約数

アクセス契約は分析ワークフローで直接作成および変更できるようになりました。

契約の表示

[View Contract] ウィンドウを起動するには、[Explore Security 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。

この表には [Policies] ウィンドウからもアクセスできます。メインメニューから次を選択します。**[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。

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

2. [Application] ドロップダウンリストから、アクションを適用するアプリケーションを選択します。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、**[+]** アイコンをクリックし、[アクション（Action）] 列と [アプリケーション（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。

新たに作成または編集した契約を保存するときに使用できるオプションは、次のとおりです。

- [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。
- [参照されているすべてのポリシーの契約を更新（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。

契約の編集

[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場合は、契約の名前の横に表示される [編集（Edit）] をクリックします。

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。

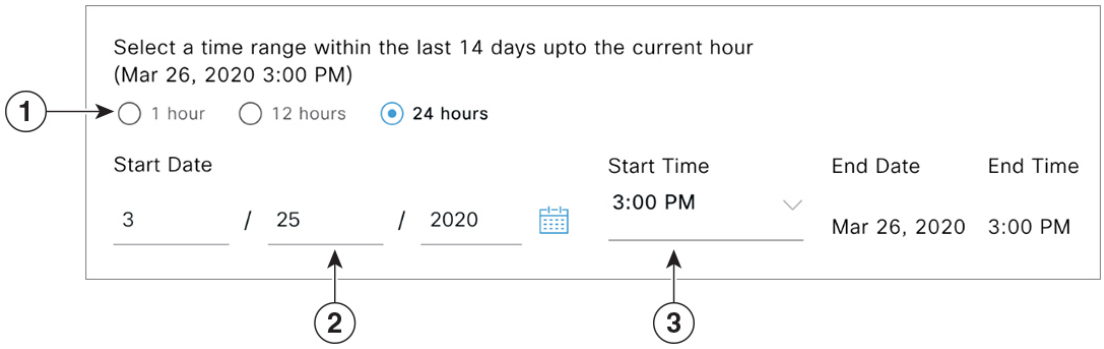
- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [参照されているすべてのポリシーの契約を更新（Update contract for all referenced policies）]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

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

接続の概要のデータを指定するために、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 *3:* 日時セレクタ



1. 次のいずれかのオプションを選択します。[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

[Overview] ウィンドウには、セキュリティグループ、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。

検索フィールドへの文字入力を開始すると、セキュリティグループ、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。MAC アドレスの場合、関連文字は 16 進数とコロンです。

Cisco グループベースポリシー分析は、エンドポイントに対し IPv4 アドレスと IPv6 アドレスの両方をサポートしています。IPv4 または IPv6 アドレスを使用してエンドポイントを検索およびフィルタリングできます。

- 次の文字を使用して、IPv4 アドレスを検索およびフィルタリングできます。
  - 数字（0 ～ 9）
  - ドット（.）

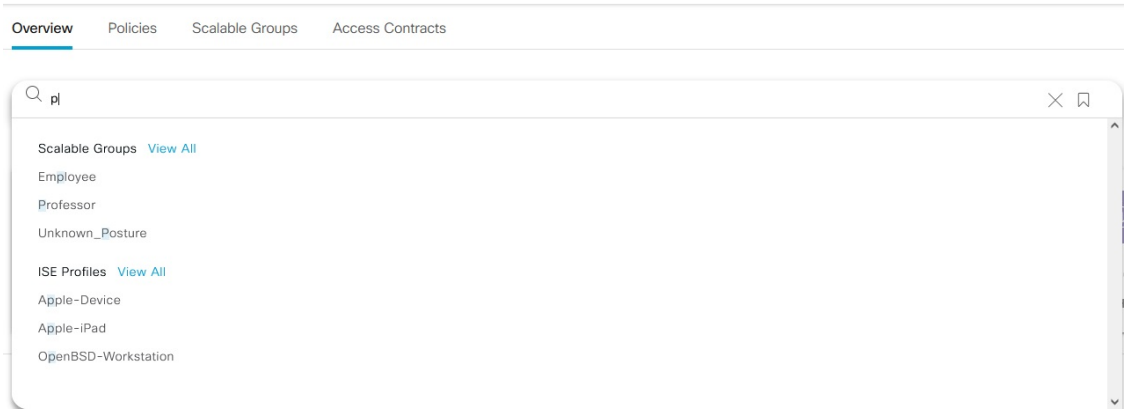
  フィルタフィールドには、最大 15 文字入力できます。
- 次の文字を使用して、IPv6 アドレスを検索およびフィルタリングできます。
  - 数字（0 ～ 9）
  - 小文字と大文字の英字（a～f、A～F）

- コロン（:）

フィルタフィールドには、最大 39 文字入力できます。

（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 （33 ページ）を参照してください。

図 *4 : [*検索（*Search***）*]* ウィンドウ**



[Focus] 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。

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。フィルタの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。

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。

ブックマークの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。

保存した検索を削除するには、ブックマークの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、十字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。

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制御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データコネクタを構成できません。
- 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。

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。

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。

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。

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。

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。

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。

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。

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。