共有オブジェクト

AWS や GCP など、クラウドベースのマネージャがオンプレミスのデータセンターとやり取りする可能性がある環境では、環境を保護するためにポリシー内でオブジェクトを共有できることが非常に重要です。共有オブジェクトを使用すると、1 ヵ所でオブジェクトを変更でき、その変更がそのオブジェクトを使用する他のすべてのポリシーに影響するため、ポリシーの維持が容易になります。共有オブジェクトを使用しない場合は、同じ変更が必要なすべてのポリシーを個別に変更する必要があります。

オブジェクトの共有は、クラウドベースのデータセンターからのトラフィックを許可するアクセス制御ポリシーを展開する場合にのみサポートされることに注意してください。ポリシーに、サードパーティのデータセンターのインスタンスまたは属性が含まれていること、または除外されていることを確認します。

Multicloud Defense はデータセンターまたはクラウドプラットフォームと通信する機能を備えているため、セキュリティポリシーをどこでも管理できます。

静的オブジェクト

静的オブジェクトは、セキュアな VPN トンネルを介して Multicloud Defense と CDO の間で共有されます。これにより、ハイブリッド環境内で同じ IP アドレスまたは FQDN を維持するオブジェクトを作成および共有できます。

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

共有中のオブジェクトの削除を選択した場合、削除は Multicloud Defense でのみ行われます。オブジェクトは CDO 内に存在し続けます。

動的オブジェクト

動的オブジェクトは、Multicloud Defense と CDO の間で共有される 1 つ以上の IP アドレスを指定するオブジェクトです。他のほとんどのオブジェクトとは異なり、動的オブジェクトを有効にするために管理対象デバイスに展開する必要はありません。元のオブジェクトに加えられた

変更は、Multicloud Defense に由来するものであるかどうかを問わず、リアルタイムで更新され、変更は次の正式な展開により直ちにプッシュされます。

CDO でコネクタを作成し、コネクタを適用可能なポリシーにアタッチしてこの機能を有効にしてから、オブジェクトをインポートして Multicloud Defense Controller で表示する必要があります。詳細については、Multicloud Defense コネクタについて （2 ページ）を参照してください。

CDO とのオブジェクトの共有

CDO でオブジェクトを共有すると、それらは自動的に**ネットワークオブジェクト**に変換されます。これは、Multicloud Defense 内のオブジェクトの元の状態には影響しません。動的オブジェクトを共有する場合は、オーバーライド値を作成してオブジェクトの元の値を保持するオプションがあります。オブジェクトのオーバーライドを使用すると、特定のデバイス上の共有ネットワークオブジェクトの値をオーバーライドできます。詳細については、『Object Overrides』を参照してください。

（注） オブジェクトは クラウド提供型 Firewall Management Center と共有できません。

- Multicloud Defense コネクタについて （2 ページ）
- CDO からのオブジェクトのインポート （2 ページ）

Multicloud Defense コネクタについて

オプションで、Cisco Secure 動的属性コネクタ に含まれるコネクタを使用して、Cisco Multicloud Defense から設定された クラウド提供型 Firewall Management Center にアドレスオブジェクトを送信できます。コネクタは、ダイナミックデータ（IP アドレスなど）を収集し、そのデータをクラウド提供型 Firewall Management Center にストリーミングして、アクセス制御ポリシーで使用できるようにします。

Multicloud Defense のオブジェクトの詳細については、「Address Objects」の章、およびアドレスオブジェクト API のドキュメントを参照してください。

Multicloud Defense コネクタの詳細については、『*Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator*』を参照してください。

CDO からのオブジェクトのインポート

（注） オブジェクトを Multicloud Defense にインポートするために、CDO ダッシュボードのダイナミック共有を有効にする必要はありません。

Multicloud Defense Controller ダッシュボードを使用して CDO オブジェクトを Multicloud Defense に手動でインポートするには、次の手順を実行します。

手順

ステップ 1 CDO にログインし、左側のペインで Multicloud Defense をクリックします。

ステップ 2 右上にある **Multicloud Defense Controller** をクリックして、コントローラダッシュボードを相互起動します。

ステップ 3 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[アドレス（Addresses）]** に移動します。

ステップ 4 [オブジェクトのインポート（Import Objects）] をクリックします。

ステップ 5 CDO オブジェクトのポップアップウィンドウから、スクロールまたは検索バーを使用して個々のオブジェクトを見つけます。

注：現時点で、Multicloud Defense では「.」を含む名前のオブジェクトはサポートされていません。名前にピリオドを含むオブジェクトを共有またはインポートしようとすると、エラーメッセージが表示されます。

ステップ 6 オブジェクトを選択して強調表示し、[インポート（Import）] をクリックします。任意の時点で [キャンセル（Cancel）] をクリックし、アクションを取り消すことができます。

次のタスク

Multicloud Defense が CDO と通信し、インポートしたオブジェクトが同期されるまで数分待ちます。CDO ダッシュボードから、更新された共有オブジェクトの数を [Multicloud Defenseの共有オブジェクト（Multicloud Defense Shared Object）] ウィジェットで確認できます。

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。