CHAPTER 10

アクセス コントロール ルール:カスタム セキュリティ グループ タグ

セキュリティ グループ タグ(SGT)は、信頼ネットワーク内におけるトラフィックの送信元の権限を指定します。ユーザが TrustSec または ISE でセキュリティ グループを追加すると、セキュリティ グループ アクセス(Cisco TrustSec と Cisco ISE の両方に共通の機能)が自動的に SGT を生成します。SGA は、パケットがネットワークに入ると、SGT 属性を適用します。ISE をアイデンティティ ソースとして設定するかまたはカスタム SGT オブジェクトを作成することで、アクセス コントロール用に SGT を使用できます。

カスタム SGT 条件により、カスタム SGT オブジェクトに基づいてアクセス コントロール ルールを設定できます。カスタム SGT オブジェクトの FirePOWER システムへの追加は、ISE を介して SGT を取得するのではなく、手動で行います。

アイデンティティ ソースとしての ISE を無効にすると、カスタム SGT 条件しか使用できなくなります。

以降のトピックでは、アクセス コントロール ルールで SGT 条件を使用する方法を説明します。

ISE SGT とカスタム SGT ルール条件との比較

ISE をアイデンティティ ソース(*ISE SGT*)として設定するかまたはカスタム SGT オブジェクト(*custom SGT*)を作成することで、アクセス コントロール用に SGT を使用できます。システムによる ISE SGT とカスタム SGT ルール条件の扱いは、次のように異なります。

ISE SGT:設定済みの ISE 接続がある

アクセス コントロール ルールでは、ISE SGT は ISE 属性条件として使用できます。[SGT/ISE Attributes]タブの [Available Attributes] リストから [Security Group Tag] を選択すると、システムは使用可能なタグを ISE に照会して、[Available Metadata]リストに入力します。パケットに SGT 属性が存在するかしないかにより、システムの応答が次のように決まります。

- SGT 属性がパケット内に存在している場合、システムはその値を抽出し、それをアクセス コントロール ルール内の ISE SGT 条件と比較します。
- SGT 属性がパケットにない場合、システムはパケットのソース IP アドレスと関連付けられている SGT が ISE で既知であるかどうかを判別し、SGT をアクセス コントロール ルール内の ISE SGT 条件と比較します。

カスタム SGT:設定済みの ISE 接続がない

カスタム SGT オブジェクトを作成し、それをアクセス コントロール ルール内の条件として使用できます。[SGT/ISE Attributes]タブの [Available Attributes] リストから [Security Group Tag] を選択すると、システムは [Available Metadata]リストに、ユーザが追加した SGT オブジェクトを入力します。パケットに SGT 属性が存在するかしないかにより、システムの応答が次のように決まります。

- SGT 属性がパケット内に存在している場合、システムはその値を抽出し、それをアクセス コントロール ルール内のカスタム SGT 条件と比較します。
- SGT 属性がパケット内にない場合、システムはパケットをアクセス コントロール ルール内のカスタム SGT 条件と照合しません。

カスタム SGT から ISE SGT ルール条件への自動移行

カスタム SGT オブジェクトを条件として使用してアクセス コントロール ルールを作成し、後で ISE をアイデンティティ ソースとして設定すると、システムは以下を行います。

- オブジェクト マネージャの [Security Group Tag]オブジェクト オプションを無効にします。ISE 接続を無効にしない限り、新規 SGT オブジェクトの追加、既存の SGT オブジェクトの編集、または新規条件としての SGT オブジェクトの追加はできません。
- 既存の SGT オブジェクトを保持します。これら既存のオブジェクトは変更できません。それらは、それらを条件として使用する既存のアクセス コントロール ルールのコンテキストでのみ表示できます。
- カスタム SGT 条件がある既存のアクセス コントロール ルールを保持します。カスタム SGT オブジェクトは手動編集でしか更新できないため、シスコはこれらのルールを削除するか、または無効にすることをお勧めしています。代わりに、SGT を ISE 属性条件として使用するルールを作成してください。システムは ISE 属性条件の SGT メタデータを更新するように ISE を自動的に照会しますが、手動編集ではカスタム SGT オブジェクトしか更新できません。

カスタム SGT 条件の設定

ライセンス:すべて

カスタム セキュリティ グループ タグ(SGT)を設定する方法:

ステップ 1　アクセス コントロール ルール エディタで、[SGT/ISE Attributes]タブをクリックします。

ステップ 2　[Available Attributes]リストから [Security Group Tag] を選択します。

ステップ 3　[Available Metadata]リストで、カスタム SGT オブジェクトを見つけて選択します。

選択すると、ルールは SGT 属性があるすべてのトラフィックと一致します。たとえば、この値は、TrustSec 向けに構成されていないホストからのトラフィックをブロックするルールが必要な場合に選択できます。

ステップ 4　[Add to Rule]をクリックするか、ドラッグ アンド ドロップします。

ステップ 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開(4-12 ページ)を参照してください。

カスタム SGT 条件のトラブルシューティング

予期しないルールの動作に気付いたら、カスタム SGT オブジェクトの設定を調整することを検討してください。

使用不可のセキュリティ グループ タグ オブジェクト

カスタム SGT オブジェクトは、ISE をアイデンティティ ソースとして設定していない場合にのみ使用できます。詳細については、カスタム SGT から ISE SGT ルール条件への自動移行（10-2 ページ）を参照してください。