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の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)により、SGT が自動的に生成されます。パケットがネットワークに入ると、SGA によって SGT 属性が適用されます。SGT をアクセス コントロールに使用するには、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します。

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。

カスタム SGT 条件を使用できるのは、アイデンティティ ソースとしての ISE/ISE-PIC を無効にしている場合のみです。

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

- ISE SGT ルール条件とカスタム SGT ルール条件との比較(10-1 ページ)
- カスタム SGT ルール条件から ISE SGT ルール条件への自動移行(10-2 ページ)
- カスタム SGT 条件の設定(10-2 ページ)
- カスタム SGT 条件のトラブルシューティング(10-3 ページ)

ISE SGT ルール条件とカスタム SGT ルール条件との比較

SGT をアクセス コントロールに使用するには、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(*カスタム SGT*)を作成します。システムによる ISE SGT ルール条件とカスタム 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

ISE SGT は、アクセス コントロール ルール内の ISE 属性条件として使用できます。[SGT/ISE 属性(SGT/ISE Attributes)] タブの [使用可能な属性(Available Attributes)] リストから [セキュリティ グループ タグ(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、[使用可能なメタデータ(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 属性(SGT/ISE Attributes)] タブの [使用可能な属性(Available Attributes)] リストから [セキュリティ グループ タグ(Security Group Tag)] を選択すると、システムは、[使用可能なメタデータ(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存在しない場合、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 ルール条件から 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 ルールを作成した後に ISE/ISE-PIC をアイデンティティ ソースとして設定した場合のシステムの動作は、次のとおりです。

- オブジェクト マネージャの [セキュリティ グループ タグ(Security Group Tag)] オブジェクト オプションを無効にします。ISE/ISE-PIC 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 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。これらの既存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 ルールとの関連で表示のみができます。
- 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、これらのルールは削除するか、または無効にすることを推奨します。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 属性条件について SGT メタデータを更新するため ISE への照会を自動的に行いますが、カスタム SGT オブジェクトは、手動編集でしか更新できません。

カスタム SGT 条件の設定

ライセンス:任意(Any)

カスタム セキュリティ グループ タグ(SGT)条件を設定する方法:

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

手順 2　[使用可能な属性(Available Attributes)] リストから [セキュリティ グループ タグ(Security Group Tag)] を選択します。

手順 3　[使用可能なメタデータ（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するようになります。たとえば、この値は、TrustSec 向けに設定されていないホストからのトラフィックをルールでブロックしたい場合に選択できます。

手順 4　[ルールに追加（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。

手順 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（4-13 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/ISE-PIC 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 ルール条件から 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。