CHAPTER 24

Cisco Security Group Access のポリシー

この章では、セキュリティ グループ アクセス（SGA）ポリシーを使用して、Cisco Identity Services Engine（Cisco ISE）ノードを認証サーバとして設定する方法について説明します。これを行うには、Cisco SGA ソリューション対応ネットワークが必要です。

この章は次のトピックで構成されています。

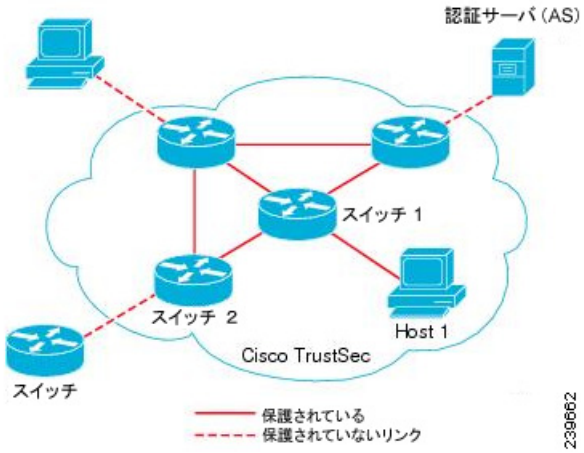
セキュリティ グループ アクセス アーキテクチャ

Cisco Security Group Access（SGA）ソリューションでは、信頼ネットワーク デバイスのクラウドを確立して、セキュアなネットワークを構築します。Cisco SGA クラウド内の個々のデバイスは、そのネイバー（ピア）によって認証されます。SGA クラウド内のデバイス間の通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。SGA ソリューションでは、認証中に取得したデバイスおよびユーザ ID 情報を使用して、ネットワークに入ってきたパケットを分類（色付け）します。このパケット分類は、パケットが SGA 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ます。エンドポイント デバイスで SGT に応じてトラフィックをフィルタリング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。

SGA サービスを有効にするには、Cisco ISE の拡張ライセンス パッケージが必要です。

図 24-1 に、SGA ネットワーク クラウドの例を示します。

図 24-1　　SGA のアーキテクチャ



関連項目

- http://www.cisco.com/en/US/netsol/ns1051/index.html
- 「SGA の機能」（P.24-2）
- 「SGA の用語」（P.24-3）
- 「SGA がサポートされているスイッチ」（P.24-4）
- 「SGA に必要なコンポーネント」（P.24-5）

SGA の機能

SGA ソリューションの主要な機能は次のとおりです。

- ネットワーク デバイス アドミッション コントロール（NDAC）：信頼ネットワークでは、認証中に、SGA クラウド内にある各ネットワーク デバイス（イーサネット スイッチなど）のクレデンシャルおよび信頼性が、そのピア デバイスによって検証されます。NDAC は IEEE 802.1x ポートベース認証を使用し、その拡張認証プロトコル（EAP）方式として Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）を使用します。NDAC プロセスの認証および許可が成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションが実行されます。
- エンドポイント アドミッション コントロール（EAC）：SGA クラウドに接続しているエンドポイント ユーザまたはデバイスの認証プロセス。EAC は一般的にアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可が成功すると、ユーザまたはデバイスに対する SGT 割り当てが実行されます。認証および許可の EAC アクセス方法には次のものがあります。
  - 802.1X ポートベースの認証
  - MAC 認証バイパス（MAB）
  - Web 認証（WebAuth）

- セキュリティ グループ（SG）：アクセス コントロール ポリシーを共有するユーザ、エンドポイント デバイス、およびリソースのグループ。SG は、管理者が Cisco ISE で定義します。新規ユーザおよびデバイスが SGA ドメインに追加されると、Cisco ISE では、これらの新規エントリを適切なセキュリティ グループに割り当てます。
- セキュリティ グループ タグ（SGT）：SGA サービスは各セキュリティ グループに、その範囲が SGA ドメイン内でグローバルな、一意のセキュリティ グループ番号（16 ビット）を割り当てます。スイッチ内のセキュリティ グループの数は、認証されたネットワーク エンティティの数に制限されます。セキュリティ グループ番号を手動で設定する必要はありません。これらは自動的に生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。
- セキュリティ グループ アクセス コントロール リスト（SGACL）：SGACL では、割り当てられている SGT に基づいてアクセスおよび権限を制御できます。権限をロールにまとめることにより、セキュリティ ポリシーの管理が容易になります。デバイスを追加するときに、1 つ以上のセキュリティ グループを割り当てるだけで、即座に適切な権限が付与されます。セキュリティ グループを変更することにより、新しい権限を追加したり、現在の権限を制限することもできます。
- セキュリティ交換プロトコル（SXP）：セキュリティ交換プロトコル（SXP）は、SGA サービス用に開発されたプロトコルで、SGT 対応ハードウェアをサポートしていないネットワーク デバイス間で、SGT/SGACL をサポートしているハードウェアに IP と SGT とのバインディング テーブルを伝播します。
- 環境データのダウンロード：SGA デバイスは、初めて信頼ネットワークに参加するときに、その環境データを Cisco ISE から取得します。デバイス上の一部のデータは、手動で設定することもできます。デバイスでは、期限切れになる前に環境データを更新する必要があります。SGA デバイスは、次の環境データを Cisco ISE から取得します。
  - サーバ リスト：クライアントがその後の RADIUS 要求に使用できるサーバのリスト（認証および許可の両方）
  - デバイス SG：そのデバイス自体が属しているセキュリティ グループ
  - 有効期間：SGA デバイスが環境データをダウンロードまたは更新する頻度を左右する期間
- SGT 予約：IP と SGT とのマッピングを有効にするために SGT の範囲を予約する、Cisco ISE の拡張機能。
- IP と SGT とのマッピング：エンドポイント IP を SGT にバインドして SGA 対応デバイスにプロビジョニングする Cisco ISE の拡張機能。Cisco ISE Release 1.2 では、IP と SGT とのマッピングの 1000 の入力がサポートされます。
- ID とポートとのマッピング：エンドポイントの接続先のポートでスイッチが ID を定義するための方法で、この ID を使用して Cisco ISE サーバ内の特定の SGT 値が検索されます。

SGA の用語

表 24-1 に、SGA ソリューションで使用される一般的な用語および SGA 環境でのそれらの意味を示します。

表 24-1　SGA の用語

用語	意味
サプリカント	信頼ネットワークへの参加を試行するデバイス。
認証	信頼ネットワークへの参加を許可する前に、各デバイスの ID を検証するプロセス。

表 24-1　SGA の用語 （続き）

用語	意味
許可	信頼ネットワーク上のリソースへのアクセスを要求しているデバイスに対し、デバイスの認証 ID に基づいてアクセスのレベルを決定するプロセス。
アクセス コントロール	各パケットに割り当てられている SGT に基づいて、パケットごとにアクセス コントロールを適用するプロセス。
セキュアな通信	信頼ネットワーク内の各リンクを経由して流れるパケットをセキュリティで保護するための、暗号化、整合性、データパス リプレイ保護のプロセス。
SGA デバイス	SGA ソリューションをサポートする Cisco Catalyst 6000 シリーズまたは Cisco Nexus 7000 シリーズのスイッチ。
SGA 対応デバイス	SGA 対応デバイスとは、SGA 対応のハードウェアとソフトウェアを備えたデバイスです。たとえば、Nexus オペレーティング システムを搭載した Nexus 7000 シリーズ スイッチなどです。
SGA シード デバイス	Cisco ISE サーバに対して直接認証を行う SGA デバイス。オーセンティケータとサプリカントの両方として機能します。
入力	Cisco SGA ソリューションが有効になっているネットワーク内の SGA 対応デバイスにパケットが初めて到達すると、SGT を使用してパケットにタグが付けられます。この信頼ネットワークへの入り口点を入力と呼びます。
出力	Cisco SGA ソリューションが有効になっているネットワーク内の最後の SGA 対応デバイスをパケットが通過すると、タグが解除されます。この信頼ネットワークからの出口点を出力と呼びます。

SGA がサポートされているスイッチ

Cisco SGA ソリューションが有効になった Cisco ISE ネットワークを設定するには、SGA ソリューションおよび他のコンポーネントをサポートするスイッチが必要です。表 24-2 に、サポートされている Cisco スイッチのプラットフォームを示します。

表 24-2　サポートされるスイッチ

サポートされている Cisco スイッチのプラットフォーム		
プラットフォーム	**オペレーティング システムのバージョン**	**要件**
Cisco Nexus 7000 シリーズ	Cisco Nexus オペレーティング システム Release 5.0.2a （注）　Cisco SGA の拡張サービス パッケージ ライセンスが必要です。	エンフォースメント ポイントとして必須
Supervisor Engine 32 か 720、または Virtual Switching System（VSS）720 を搭載した Cisco Catalyst 6500E スイッチ	Cisco IOS ソフトウェア Release 12.2(33) SXI3 以降	アクセス スイッチとして任意
Cisco Catalyst 4900 シリーズ スイッチ	Cisco IOS ソフトウェア Release 2.2(50) SG7 以降	アクセス スイッチとして任意
Supervisor 6L-E または 6-E を搭載した Cisco Catalyst 4500E スイッチ	Cisco IOS ソフトウェア Release 12.2(50) SG7 以降	アクセス スイッチとして任意

表 24-2　サポートされるスイッチ （続き）

サポートされている Cisco スイッチのプラットフォーム		
Cisco Catalyst 3750-X または 3560-X シリーズ スイッチ	Cisco IOS ソフトウェア Release 12.2(53) SE1 以降	アクセス スイッチとして任意
Cisco Catalyst 3750 または 3560 シリーズ スイッチ	Cisco IOS ソフトウェア Release 12.2(53) SE1 以降	アクセス スイッチとして任意
Cisco Catalyst ブレード スイッチ 3000 または 3100 シリーズ	Cisco IOS ソフトウェア Release 12.2(53) SE1 以降	アクセス スイッチとして任意

SGA に必要なコンポーネント

表 24-2 に示されているスイッチ以外に、IEEE 802.1X プロトコルを使用した ID ベースのユーザ アクセス コントロールには、その他のコンポーネントが必要です。Microsoft Active Directory が稼働している Microsoft Windows 2003 または 2008 サーバ、認証局（CA）サーバ、ドメイン ネーム システム（DNS）サーバ、およびダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバなどです。Microsoft Windows オペレーティング システムが稼働しているエンド ホストをこの環境に含めることもできます。表 24-3 に、Cisco SGA 環境に必要となる可能性のあるその他のコンポーネントを示します。

表 24-3　コンポーネント

コンポーネント	説明
ユーザ ID リポジトリ	Cisco ISE の内部ユーザ データベースを使用することもできますが、ID 認証には外部データベースを使用することを推奨します。Cisco ISE では、Microsoft Active Directory および Lightweight Directory Access Protocol（LDAP）サービスへの接続がサポートされています。
DHCP サービス	DHCP サービスを提供する DHCP サーバ。たとえば、Microsoft Windows Server 2008 DHCP サーバなどです。
DNS サービス	DNS サービスを提供する DNS サーバ。たとえば、Microsoft Windows Server 2008 DNS サーバなどです。
認証権限サーバ	標準の CA サービスを提供する認証権限サーバ。たとえば、Microsoft Windows Server 2008 CA サーバなどです。
ターゲット サーバ	HTTP、FTP、セキュア シェル（SSH）、さらには SGACL をテストするファイル共有などのインターネット サービスを提供するサーバ
エンドポイント PC	SGA はサプリカントにとらわれないソリューションで、エンドポイント PC で稼働する特定のエージェントまたは IEEE 802.1X サプリカントを必要としません。Cisco Secure Services Client サプリカント、Microsoft Windows または別のオペレーティング システムに組み込みのサプリカント、またはその他のサードパーティ製サプリカントを使用できます

Cisco ISE を SGA 展開と相互運用できるようにするには、スイッチの SGA スイッチ ポートを設定する必要があります。

関連項目

「Cisco セキュリティ グループ アクセス スイッチ ポートの有効化」（P.F-6）

SGA ソリューションの有効化

ここでは、Cisco ISE ネットワークで SGA ソリューションを有効にするために実行する必要がある作業について説明します。

この項の構成は、次のとおりです。

スイッチでの SGA の設定

Cisco ISE を SGA 展開と相互運用できるようにするには、スイッチの SGA スイッチ ポートを設定する必要があります。詳細については、「Cisco セキュリティ グループ アクセス スイッチ ポートの有効化」（P.F-6）を参照してください。

Cisco ISE での SGA の設定に加えて、SGA デバイスでもいくつかの設定が必要です。これらの設定は Catalyst スイッチと Nexus スイッチとで異なり、次の URL で入手可能な Catalyst および Nexus スイッチ設定ガイドに記載されています。

- Catalyst 6500 シリーズ スイッチの場合：
  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html
- Nexus 7000 シリーズ スイッチの場合：

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5.x.html
- Nexus 7000 シリーズ スイッチを使用した設定例：

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/configuration_examples/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Configuration_Examples_Release_5.x_chapter4.html#con_1191129

SGA デバイスの設定

Cisco ISE で SGA 対応デバイスからの要求を処理するには、これらの SGA 対応デバイスを Cisco ISE で定義しておく必要があります。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　ネットワーク デバイスを展開に追加します。

ステップ 3　[送信（Submit）] をクリックし、SGA デバイス定義を保存します。

次の作業

- 「セキュリティ グループ アクセスの設定」（P.24-7）

関連項目

- 「ネットワーク デバイス定義の設定」（P.A-39）
- 「SGA デバイス属性の設定」（P.A-43）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

セキュリティ グループ アクセスの設定

Cisco ISE が SGA サーバとして機能して SGA サービスを提供するには、いくつかのグローバル SGA 設定を定義する必要があります。

はじめる前に

- グローバル SGA 設定の前に、グローバル EAP-FAST 設定の定義が完了していることを確認します（[管理（Administration）] > [システム（System）] > [グローバル オプション（Global Options）] > [プロトコル設定（Protocol Settings）] > [EAP-FAST] > [EAP-FAST 設定（EAP-FAST Settings）] を選択します）。

  [機関識別情報の説明（Authority Identity Info Description）] を Cisco ISE サーバ名に変更する必要があります。この説明は、クレデンシャルをエンドポイント クライアントに送信する Cisco ISE サーバを説明したわかりやすい文字列にします。Cisco SGA アーキテクチャのクライアントには、IEEE 802.1X 認証の EAP 方式として EAP-FAST を実行するエンドポイント、または NDAC を実行するサプリカント ネットワーク デバイスのいずれも使用できます。クライアントは、この文字列を Protected Access Credentials（PAC）Type-Length-Value（TLV）情報で認識できます。デフォルト値は [Cisco Identity Services Engine] です。NDAC 認証時に、ネットワーク デバイスで Cisco ISE PAC 情報が一意に識別されるように、この値を変更する必要があります。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ グループ アクセス（Security Group Access）] を選択します。

ステップ 2　フィールドに値を入力します。

ステップ 3　[保存（Save）] をクリックします。

次の作業

- 「セキュリティ グループ アクセス AAA サーバの設定」（P.24-8）

関連項目

- 「セキュリティ グループのデバイスへのマッピング」（P.24-11）
- 「セキュリティ グループ アクセス設定」（P.A-26）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

セキュリティ グループ アクセス AAA サーバの設定

展開内の Cisco ISE サーバのリストを AAA サーバ リストに設定して、これらの任意のサーバに対して SGA デバイスの認証が行われるようにできます。このリストに Cisco ISE サーバを追加すると、これらすべてのサーバの詳細が SGA デバイスにダウンロードされます。SGA デバイスは、認証を試行するときに、このリストから Cisco ISE サーバを選択します。最初のサーバがダウン状態またはビジー状態の場合、SGA デバイスはこのリストにある別の任意のサーバに対して自分自身の認証を行うことができます。デフォルトでは、プライマリ Cisco ISE サーバは SGA AAA サーバです。1 つのサーバがビジー状態の場合に、このリストの別のサーバで SGA 要求を処理できるように、この AAA サーバ リスト内に追加の Cisco ISE サーバを設定することを推奨します。

このページには、SGA AAA サーバとして設定した展開内の Cisco ISE サーバがリストされます。

[プッシュ（Push）] ボタンをクリックすると、複数の SGA AAA サーバを設定した後に、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての SGA ネットワーク デバイスに送信され、変更されたすべての SGA AAA サーバの更新が提供されます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [SGA AAA サーバ（SGA AAA Servers）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　次の説明に従って値を入力します。

- [名前（Name）] : この AAA サーバ リスト内で Cisco ISE サーバに割り当てる名前。この名前は、Cisco ISE サーバのホスト名と異なっていてもかまいません。
- [説明（Description）] : 説明（任意）。
- [IP] : AAA サーバ リストに追加する Cisco ISE サーバの IP アドレス。
- [ポート（Port）] : SGA デバイスとサーバ間の通信が実行されるポート。デフォルトは 1812 です。

ステップ 4　[送信（Submit）] をクリックします。

次の作業

「セキュリティ グループの設定」（P.24-8）

関連項目

「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

セキュリティ グループの設定

セキュリティ グループ（SG）またはセキュリティ グループ タグ（SGT）は、SGA ポリシー設定で使用される要素です。SGT は、パケットが信頼ネットワーク内を移動する場合に付加されます。これらのパケットは、信頼ネットワークに入ったとき（入力）にタグ付けされ、信頼ネットワークから離れるとき（出力）にタグ解除されます。

SGT は順次的な方法で自動的に生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。Cisco ISE は、SGT の生成時に予約済みの番号をスキップします。

特定のセキュリティ グループを削除した場合、このセキュリティ グループに割り当てられている SGT は、後続の SGT がすべて削除されるまで再利用されません。

たとえば、SGT 2、3、および 4 が定義されていて SGT 2 を削除した場合、次に生成される SGT は SGT 5 になります。SGT 2 が次に生成されるようにする場合は、SGT 3 および 4 を削除する必要があります。

SGA サービスはこれらの SGT を使用して、出力時に SGA ポリシーを適用します。

管理者ポータルの次のページからセキュリティ グループを設定できます。

- [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティ グループ アクセス（Security Group Access）] > [セキュリティ グループ（Security Groups）]。「セキュリティ グループの追加」（P.24-9）を参照してください。
- [出力ポリシー（egress policy）] ページから直接設定できます。「出力ポリシーからの SGT の設定」（P.24-16）を参照してください。
- [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティ グループ アクセス（Security Group Access）] > [セキュリティ グループ（Security Groups）] ページで、[SGT の生成（Generate SGT）] ボタンをクリックします。「セキュリティ グループの追加」（P.24-9）を参照してください。

[プッシュ（Push）] ボタンをクリックすると、複数の SGT を更新した後に、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての SGA ネットワーク デバイスに送信され、変更されたすべての SGT の更新が提供されます。

関連項目

- 「セキュリティ グループの追加」（P.24-9）
- 「デバイスへの SGT 割り当てによる SGA ポリシーの設定」（P.24-12）

セキュリティ グループの追加

SGA ソリューション内の個々のセキュリティ グループに一意の SGT を割り当てる必要があります。Cisco ISE では 65,535 SGT までサポートされていますが、SGT の数を少なくすると、SGA ソリューションをより簡単に展開および管理できるようになります。最大で 64000 SGT までにすることを推奨します。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティ グループ アクセス（Security Group Access）] > [セキュリティ グループ（Security Groups）] を選択します。

ステップ 2　[追加（Add）] をクリックして新規セキュリティ グループを追加します。

ステップ 3　フィールドに値を入力します。

ステップ 4　[保存（Save）] をクリックしてセキュリティ グループを保存します。

次の作業

- 「セキュリティ グループ アクセス コントロール リストの設定」（P.24-10）
- 「ユーザおよびエンドポイントへのセキュリティ グループの割り当て」（P.24-13）

関連項目

「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

セキュリティ グループ アクセス コントロール リストの設定

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、SGA ポリシー評価後に割り当てられる権限です。SGACL によって、IP アドレスまたはサブネット マスクのみではなく、ユーザのロールに基づいて、ユーザが実行できる操作が制限されます。管理者ポータルで SGACL を設定できます。

[プッシュ（Push）] ボタンをクリックすると、複数の SGACL を更新した後に、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての SGA ネットワーク デバイスに送信され、変更されたすべての SGACL の更新が提供されます。

関連項目

- 「セキュリティ グループ アクセス コントロール リストの追加」（P.24-10）
- 「出力ポリシーからの SGT の設定」（P.24-16）

セキュリティ グループ アクセス コントロール リストの追加

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティ グループ アクセス（Security Group Access）] > [セキュリティ グループ ACL（Security Group ACLs）] を選択します。

ステップ 2　次の情報を入力します。

- [名前（Name）]：SGACL の名前
- [説明（Description）]：SGACL の説明（任意）
- [IP バージョン（IP Version）]：この SGACL でサポートされる IP バージョン：
  - [IPv4]：IP バージョン 4（IPv4）がサポートされます
  - [IPv6]：IP バージョン 6（IPv6）がサポートされます
  - [両方（Agnostic）]：IPv4 と IPv6 の両方がサポートされます
- [セキュリティ グループ ACL コンテンツ（Security Group ACL Content）]：アクセス コントロール リスト（ACL）コマンド。次に例を示します。

  permit icmp

  deny all

ステップ 3　[送信（Submit）] をクリックします。

Nexus 7000 シリーズのアクセス コントロール リスト エントリ

Cisco Nexus オペレーティング システム 4.2 を搭載している Nexus 7000 シリーズでは、次のアクセス コントロール リスト エントリがサポートされています。

deny all

deny icmp

deny igmp

deny ip

deny tcp [{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

deny udp[{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

permit all

permit icmp

permit igmp

permit ip

permit tcp [{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

permit udp[{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

SGACL ACE、SGACL 名、または SGACL の IP バージョンを変更した場合、[プッシュ（Push）] をクリックすることで、累積されたすべての変更を SGA ネットワーク デバイスにプッシュできます。

次の作業

「デバイスへの SGT 割り当てによる SGA ポリシーの設定」（P.24-12）

関連項目

- http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/command/reference/sec_cmds_d.html#wp1057446
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」
- 「RBACL 名前付きリストの更新 CoA」（P.24-25）

セキュリティ グループのデバイスへのマッピング

Cisco ISE では、デバイスのホスト名または IP アドレスがわかっている場合に、SGA デバイスに SGT を割り当てることができます。特定のホスト名または IP アドレスを持つデバイスがネットワークに参加すると、Cisco ISE によって認証前に SGT が割り当てられます。このマッピングは [セキュリティ グループ マッピング（Security Group Mappings）] ページから作成できます。この操作を実行する前に、SGT の範囲が予約済みであることを確認します。管理者ポータルからセキュリティ グループをデバイスにマッピングできます。

関連項目

- 「セキュリティ グループ マッピングの追加」（P.24-11）
- 「セキュリティ グループ アクセスの設定」（P.24-7）

セキュリティ グループ マッピングの追加

管理者ポータルからセキュリティ グループ マッピングを追加できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティ グループ マッピング（Security Group Mappings）] を選択します。

ステップ 2　[追加（Add）] をクリックして新規セキュリティ グループ マッピングを追加します。

ステップ 3　フィールドに値を入力します。

ステップ 4　再割り当てする既存のセキュリティ グループ マッピングの隣にあるチェックボックスをオンにし、[グループの再割り当て（Reassign Groups）] をクリックします。

ステップ 5　展開する既存のセキュリティ グループ マッピングの隣にあるチェックボックスをオンにし、[展開（Deploy）] をクリックします。

ステップ 6　ステータスを確認する既存のセキュリティ グループ マッピングの隣にあるチェックボックスをオンにし、[>>] を選択してから [ステータスの確認（Check Status）] をクリックします。

ステップ 7　[送信（Submit）] をクリックします。

関連項目

「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

デバイスへの SGT 割り当てによる SGA ポリシーの設定

SGT をデバイスに割り当てることによって SGA ポリシーを設定できます。SGA デバイス ID を使用することで、セキュリティ グループをデバイスに割り当てることができます。

はじめる前に

- ポリシーで使用するセキュリティ グループを作成していることを確認します。詳細については、「セキュリティ グループの設定」（P.24-8）を参照してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [セキュリティ グループ アクセス（Security Group Access）] > [ネットワーク デバイス許可（Network Device Authorization）] を選択します。

ステップ 2　[デフォルト ルール（Default Rule）] 行の [操作（Action）] アイコンをクリックし、[新規行を上に挿入（Insert New Row Above）] をクリックします。

ステップ 3　このルールの名前を入力します。

ステップ 4　[条件（Conditions）] の隣にあるプラス記号（+）をクリックして、ポリシー条件を追加します。

ステップ 5　[新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）] をクリックし、新しい条件を作成できます。

ステップ 6　[セキュリティ グループ（Security Group）] ドロップダウン リストから、この条件の評価が true になった場合に割り当てる SGT を選択します。

ステップ 7　この行の [操作（Action）] アイコンをクリックして、現在のルールの上または下に、デバイス属性に基づいた別のルールを追加します。この処理を繰り返して、SGA ポリシーに必要なすべてのルールを作成できます。ルールをドラッグ アンド ドロップし、  アイコンをクリックすることでこれらの順序を変更できます。既存の条件を複製することもできますが、ポリシー名は必ず変更してください。

評価が true になる最初のルールによって、評価の結果が決まります。いずれのルールも一致しなかった場合、デフォルト ルールが適用されます。デフォルト ルールを編集して、いずれのルールも一致しなかった場合にデバイスに適用される SGT を指定できます。

ステップ 8　[保存（Save）] をクリックして SGA ポリシーを保存します。

ネットワーク デバイス ポリシーを設定した後に、SGA デバイスで認証を行おうとすると、デバイスはその SGT およびそのピアの SGT を取得し、関連するすべての詳細をダウンロードできるようになります。

関連項目

「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

ユーザおよびエンドポイントへのセキュリティ グループの割り当て

Cisco ISE では、許可ポリシー評価の結果としてセキュリティ グループを割り当てることができます。このオプションを使用すると、ユーザおよびエンドポイントにセキュリティ グループを割り当てることができます。

はじめる前に

- 許可ポリシーについては、「Cisoc ISE の許可プロファイル」（P.20-1）を参照してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[ポリシー（Policy）] > [許可（Authorization）] > [標準（Standard）] を選択します。

ステップ 2　新しい許可ポリシーを作成します。

ステップ 3　[権限（Permissions）] で、許可プロファイルを選択する代わりにセキュリティ グループを選択します。

あるユーザまたはエンドポイントについて、この許可ポリシーで指定した条件が true の場合、このセキュリティ グループがそのユーザまたはエンドポイントに割り当てられ、このユーザまたはエンドポイントによって送信されたすべてのデータ パケットにこの特定の SGT でタグが付けられます。

関連項目

- 「許可ポリシーの設定」（P.20-8）
- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

出力ポリシー

出力テーブルには、送信元 SGT および宛先 SGT が、予約済みのものもそうでないものもあわせてリストされます。また、このページでは、出力テーブルをフィルタリングして特定のポリシーを表示することや、カスタム ビューを保存することもできます。送信元 SGT から宛先 SGT に到達しようとすると、SGA 対応デバイスは、出力ポリシーで定義されている SGA ポリシーに基づいて SGACL を適用します。Cisco ISE はポリシーを作成してプロビジョニングします。

SGA ポリシーの作成に必要な基本的構築ブロックである SGT および SGACL を作成した後に、SGACL を送信元 SGT および宛先 SGT に割り当てることによって、それらの関係を確立できます。

送信元 SGT と宛先 SGT のそれぞれの組み合わせが、出力ポリシーのセルになります。

この項の構成は、次のとおりです。

関連項目

- 「セキュリティ グループの設定」（P.24-8）
- 「セキュリティ グループ アクセス コントロール リストの設定」（P.24-10）

出力ポリシーの表示

[ポリシー（Policy）] > [セキュリティ グループ アクセス（Security Group Access）] > [出力ポリシー（Egress Policy）] ページで出力ポリシーを表示できます。

それぞれ異なる 3 つの方法で出力ポリシーを表示できます。

送信元ツリー

送信元ツリー ビューには、簡潔で組織化された送信元 SGT のビューが折りたたまれた状態で表示されます。送信元 SGT を展開すると、選択した送信元 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、宛先 SGT にマッピングされている送信元 SGT のみが表示されます。特定の送信元 SGT を展開すると、この送信元 SGT にマッピングされているすべての宛先 SGT とその設定がテーブルに表示されます。

一部のフィールドの隣に 3 つのドット（...）が表示されます。これは、セルに詳細情報が含まれていることを意味します。カーソルを 3 つのドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

宛先ツリー

宛先ツリー ビューには、簡潔で組織化された宛先 SGT のビューが折りたたまれた状態で表示されます。宛先 SGT を展開すると、選択した宛先 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、送信元 SGT にマッピングされている宛先 SGT のみが表示されます。特定の宛先 SGT を展開すると、この宛先 SGT にマッピングされているすべての送信元 SGT とその設定がテーブルに表示されます。

一部のフィールドの隣に 3 つのドット（...）が表示されます。これは、セルに詳細情報が含まれていることを意味します。カーソルを 3 つのドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

マトリクス ビュー

出力ポリシーのマトリクス ビューは、スプレッドシートに似ています。ここには 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 SGT がリストされます。
- 宛先軸：水平軸にはすべての宛先 SGT がリストされます。

送信元 SGT と宛先 SGT のマッピングが、セルとして示されます。セルにデータが含まれている場合、対応する送信元 SGT と宛先 SGT 間にマッピングがあるということになります。マトリクス ビューには 2 つのタイプのセルがあります。

- マッピングされたセル：送信元 SGT と宛先 SGT のペアが、順序付けされた SGACL のセットに関連付けられ、特定のステータスになっている場合。
- マッピングされていないセル：送信元 SGT と宛先 SGT のペアが、SGACL に関連付けられてなく、特定のステータスになっていない場合。

出力ポリシー セルには、送信元 SGT、宛先 SGT、最終的な catch-all ルールが 1 つのリストとして SGACL の下にカンマで区切られて表示されます。最終的な catch-all ルールは、[なし（None）] に設定されている場合には表示されません。マトリクス内の空のセルは、マッピングされていないセルを示します。

出力ポリシーのマトリクス ビューでは、マトリクスをスクロールして目的のセルのセットを表示できます。ブラウザがマトリクス データ全体を一度にロードすることはありません。ブラウザは、ユーザがスクロールした領域に移入されるデータをサーバに要求します。これにより、メモリのオーバーフローおよびパフォーマンスの問題を防ぐことができます。

関連項目

「マトリクス操作」（P.24-15）

マトリクス操作

Cisco ISE のマトリクス ビューは、スプレッドシートに似ています。行のタイトルとして発信元 SGT、カラムのタイトルとして宛先 SGT が含まれます。セルは、送信元 SGT と宛先 SGT の交差部分です。マトリクス ビューのセルには、送信元および宛先のペアと SGACL との設定情報が含まれます。マトリクス ビューでは、セル領域を節約するために、すべてのフィールドが表示されることはありません。

マトリクスでの移動

カーソルでマトリクス 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、マトリクス内を移動できます。セルをクリックしたままにし、マトリクス コンテンツ全体を任意の方向にドラッグできます。送信元および宛先のバーがセルと一緒に移動します。セルを選択すると、マトリクス ビューによってそのセルと対応する行（送信元 SGT）およびカラム（宛先 SGT）が強調表示されます。選択したセルの座標（送信元 SGT および宛先 SGT）がマトリクス コンテンツ領域の下に表示されます。

マトリクスでのセルの選択

マトリクス ビューでセルを選択するには、該当のセルをクリックします。選択したセルが別の色で表示され、送信元 SGT および宛先 SGT が強調表示されます。セルをもう一度クリックするか、または別のセルを選択することで、セルの選択を解除できます。複数セルの選択は、マトリクス ビューでは許可されていません。セルをダブルクリックして、セルの設定を編集します。

出力ポリシー テーブル セルの設定

Cisco ISE では、ツールバーで使用可能なさまざまなオプションを使用して、セルを設定できます。Cisco ISE では、選択した送信元 SGT および宛先 SGT がマッピングされたセルと同一である場合には、セルを設定できません。

ここでは、次の内容について説明します。

- 「出力ポリシー セルのマッピングの追加」（P.24-16）
- 「出力ポリシーからの SGT の設定」（P.24-16）

出力ポリシー セルのマッピングの追加

[ポリシー（Policy）] ページから出力ポリシーのマッピング セルを追加できます。

ステップ 1　[ポリシー（Policy）] > [セキュリティ グループ アクセス（Security Group Access）] > [出力ポリシー（Egress Policy）] を選択します。

ステップ 2　適切なビューのタブをクリックして、マトリクス セルを表示します。

ステップ 3　マトリクス セルを選択するには、次の手順を実行します。

- マトリクス ビューで、セルをクリックして選択します。
- 送信元ツリー ビューおよび宛先ツリー ビューで、内部テーブル内の行のチェックボックスをオンにして選択します。

ステップ 4　新しいマッピング セルを追加するには [追加（Add）] をクリックします。

ステップ 5　次の項目について適切な値を選択します。

- 送信元セキュリティ グループ（Source Security Group）
- 宛先セキュリティ グループ（Destination Security Group）
- ステータス（Status）、セキュリティ グループ ACL（Security Group ACLs）
- 最終的な catch-all ルール（Final Catch All Rule）

ステップ 6　設定を保存するには、[送信（Submit）] をクリックします。

出力ポリシーからの SGT の設定

[出力ポリシー（Egress Policy）] ページからセキュリティ グループを直接作成できます。

ステップ 1　[ポリシー（Policy）] > [セキュリティ グループ アクセス（Security Group Access）] > [出力ポリシー（Egress Policy）] を選択します。

ステップ 2　[設定（Configure）] オプション ドロップダウン リストから [セキュリティ グループの作成（Create Security Group）] を選択します。

ステップ 3　セキュリティ グループを作成します。

関連項目

「セキュリティ グループの設定」（P.24-8）

出力ポリシーからの SGACL の設定

[出力ポリシー（Egress Policy）] ページからセキュリティ グループ ACL を直接作成できます。

ステップ 1　[ポリシー（Policy）] > [セキュリティ グループ アクセス（Security Group Access）] > [出力ポリシー（Egress Policy）] を選択します。

ステップ 2　[設定（Configure）] オプション ドロップダウン リストから [セキュリティ グループ ACL の作成（Create Security Group ACLs）] を選択します。

ステップ 3　セキュリティ グループ ACL を作成します。

関連項目

「セキュリティ グループ アクセス コントロール リストの設定」（P.24-10）

[プッシュ（Push）] ボタン

出力ポリシーの [プッシュ（Push）] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの出力ポリシー設定変更に関する更新を、ただちに要求するよう SGA デバイスに伝えます。

関連項目

「SGT マトリクスの更新 CoA」（P.24-26）

モニタ モード

出力ポリシーの [すべてをモニタ（Monitor All）] オプションを使用すると、出力ポリシー設定ステータス全体を 1 回のクリックでモニタ モードに変更できます。[出力ポリシー（egress policy）] ページの [すべてをモニタ（Monitor All）] チェックボックスをオンにして、すべてのセルの出力ポリシー設定ステータスをモニタ モードに変更します。[すべてをモニタ（Monitor All）] チェックボックスをオンにすると、設定ステータスが次のように変更されます。

- ステータスが [有効（Enabled）] であるセルはモニタ対象として動作しますが、有効であるかのように表示されます。
- ステータスが [無効（Disabled）] であるセルは何も影響を受けません。
- ステータスが [モニタ（Monitor）] であるセルは、[モニタ対象（Monitored）] のままになります。

[すべてをモニタ（Monitor All）] チェックボックスをオフにすると、元の設定ステータスに戻ります。データベース内の実際のセルのステータスは変更されません。[すべてをモニタ（Monitor All）] をオフにすると、出力ポリシーのそれぞれのセルが元の設定ステータスに戻ります。

モニタ モードの機能

モニタ モードのモニタリング機能は次の操作に役立ちます。

- フィルタリングされているけれども、モニタ モードではモニタされているトラフィックの量の確認
- SGT-DGT ペアがモニタ モードであるか強制モードであるかの確認と、ネットワーク内で異常なパケット ドロップが発生していないかどうかの観察

- SGACL ドロップが実際に強制モードによって強制されているのか、またはモニタ モードによって許可されているのかの確認
- モードのタイプ（モニタ、強制、または両方）に基づいたカスタム レポートの作成
- NAD に適用されている SGACL、および表示の不一致（ある場合）の識別

関連項目

- ユーザ別上位 N 個の RBACL ドロップの実行
- 第 26 章「レポート」

ユーザ別上位 N 個の RBACL ドロップの実行

ユーザ別上位 N 個の RBACL ドロップ レポートを次のように実行できます。

ステップ 1　Cisco ISE 管理ダッシュボードで、[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [セキュリティ グループ アクセス（Security Group Access）] を選択します。

ステップ 2　[ユーザ別上位 N 個の RBACL ドロップ（Top N RBACL Drops by User）] をクリックします。

ステップ 3　[フィルタ（Filters）] ドロップダウン メニューから必要なモニタ モードを追加します。次のオプションを使用できます。

- 宛先名（Destination Name）/ 宛先アドレス（Destination Address）
- SGA SGT
- SGA DGT
- 強制モード（Enforcement Mode）

ステップ 4　選択したパラメータに適宜値を入力します。[強制モード（Enforcement mode）] ドロップダウン リストからモードを [強制（Enforce）]、[モニタ（Monitor）]、または [両方（Both）] として指定できます。

ステップ 5　[時間範囲（Time Range）] ドロップダウン メニューから、レポート データを収集する時間を選択します。

ステップ 6　指定した期間に、選択したパラメータでレポートを実行するには、[実行（Run）] をクリックします。

不明セキュリティ グループ

不明セキュリティ グループは事前に設定されているセキュリティ グループで、変更不可能であり、ox000 SGT を表します。

Cisco Security Group ネットワーク デバイスは、送信元または宛先のいずれかの SGT がない場合に不明 SGT を参照するセルを要求します。送信元のみが不明の場合、要求は <不明, 宛先 SGT> セルに適用されます。宛先のみが不明の場合、要求は <送信元 SGT, 不明> セルに適用されます。送信元および宛先の両方が不明の場合、要求は <不明, 不明> セルに適用されます。

デフォルト ポリシー

デフォルト ポリシーは、<ANY,ANY> セルを参照します。任意の送信元 SGT が任意の宛先 SGT にマッピングされています。ここでは、ANY SGT は変更不可能であり、送信元 SGT にも宛先 SGT にも表示されません。ANY SGT は ANY SGT とのみペアにできます。他の SGT とはペアにできません。SGA ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

- つまり、セルが空白の場合は、デフォルト ポリシーのみが含まれることになります。
- セルにポリシーが含まれる場合、結果のポリシーは、セル固有のポリシーとその後に続くデフォルト ポリシーの組み合わせになります。

Cisco ISE では、セル ポリシーおよびデフォルト ポリシーは 2 つの別々の SGACL セットになり、デバイスは 2 つの別々のポリシー クエリーの応答としてこれらのセットを取得します。

デフォルト ポリシーの設定は、他のセルと次の点で異なります。

- ステータスは [有効（Enabled）] または [モニタ対象（Monitored）] の 2 つの値しかとることができません。
- セキュリティ グループ ACL は、デフォルト ポリシーでは任意のフィールドであるため、空白のままにできます。
- 最終的な catch-all ルールは、[許可 IP（Permit IP）] または [拒否 IP（Deny IP）] のいずれかにできます。デフォルト ポリシーを上回る安全策はないため、ここで [なし（None）] オプションを使用できないことは明らかです。

OOB SGA PAC

すべての SGA ネットワーク デバイスで、EAP-FAST プロトコルの一部として SGA PAC が保持されています。これはセキュアな RADIUS プロトコルでも使用され、ここでは RADIUS 共有秘密が PAC で伝送されるパラメータから作成されます。これらのパラメータの 1 つである発信側 ID には、SGA ネットワーク デバイス ID、つまりデバイス ID が保持されます。

デバイスが SGA PAC を使用して識別される場合、Cisco ISE でそのデバイス用に設定されているデバイス ID と、PAC の発信側 ID が一致していない場合、認証に失敗します。

一部の SGA デバイス（Cisco ファイアウォール ASA など）では EAP-FAST プロトコルをサポートしていません。したがって、Cisco ISE ではこれらのデバイスを EAP-FAST を介した SGA PAC でプロビジョニングできません。代わりに、SGA PAC は Cisco ISE 上で生成され、手動でデバイスにコピーされます。そのため、これをアウトオブバンド（OOB）SGA PAC 生成と呼びます。

Cisco ISE で PAC を生成すると、暗号キーで暗号化された PAC ファイルが生成されます。

ここでは、次の内容について説明します。

- 「SGA PAC プロビジョニング」（P.24-19）
- 「SGA PAC のモニタリング」（P.24-21）

SGA PAC プロビジョニング

ここでは、次の内容について説明します。

- 「[設定（Settings）] 画面からの SGA PAC の生成」（P.24-19）
- 「[ネットワーク デバイス（Network Devices）] 画面からの SGA PAC の生成」（P.24-20）
- 「[ネットワーク デバイス リスト（Network Devices List）] 画面からの SGA PAC の生成」（P.24-20）

[設定（Settings）] 画面からの SGA PAC の生成

[設定（Settings）] 画面から SGA PAC を生成できます。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] を選択します。

ステップ 2　左側の [設定（Settings）] ナビゲーション ペインで [プロトコル（Protocols）] をクリックします。

ステップ 3　[EAP-FAST] > [PAC の生成（Generate PAC）] を選択します。

ステップ 4　SGA PAC を生成します。

関連項目

「EAP-FAST の PAC の生成」（P.19-13）

[ネットワーク デバイス（Network Devices）] 画面からの SGA PAC の生成

[ネットワーク デバイス（Network Devices）] 画面から SGA PAC を生成できます。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　[追加（Add）] をクリックします。または、[ネットワーク デバイス（Network Devices）] ナビゲーション ペインのアクション アイコンで [新規デバイスの追加（Add new device）] をクリックします。

ステップ 3　新規デバイスを追加する場合は、デバイス名を入力します。

ステップ 4　[セキュリティ グループ アクセス（SGA）（Security Group Access (SGA)）] チェックボックスをオンにして、SGA デバイスを設定します。

ステップ 5　[アウトオブバンド（OOB）SGA PAC（Out of Band (OOB) SGA PAC）] サブ セクションで、[PAC の生成（Generate PAC）] をクリックします。

ステップ 6　次の詳細事項を入力します。

- [PAC 存続可能時間（PAC Time to Live）] : 日、週、月、年の単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
- [暗号化キー（Encryption Key）] : 暗号化キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーには、大文字や小文字、数字、または英数字の組み合わせを含めることができます。

暗号キーを使用して、生成されるファイルの PAC が暗号化されます。このキーは、デバイスで PAC ファイルを復号化する場合にも使用されます。したがって、後で使用できるように管理者が暗号キーを保存しておくことを推奨します。

[ID（Identity）] フィールドは SGA ネットワーク デバイスのデバイス ID を示し、このフィールドには EAP-FAST プロトコルによって発信側 ID が提供されます。ここで入力した ID 文字列がそのデバイス ID と一致しない場合、認証は失敗します。

有効期限は、PAC 存続可能時間に基づいて計算されます。

ステップ 7　[PAC の生成（Generate PAC）] をクリックします。

[ネットワーク デバイス リスト（Network Devices List）] 画面からの SGA PAC の生成

[ネットワーク デバイス リスト（Network Devices list）] 画面から SGA PAC を生成できます。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　[ネットワーク デバイス（Network Devices）] をクリックします。

ステップ 3　SGA PAC を生成するデバイスの隣にあるチェックボックスをオンにし、[PAC の生成（Generate PAC）] をクリックします。

ステップ 4　フィールドに詳細を入力します。

ステップ 5　[PAC の生成（Generate PAC）] をクリックします。

関連項目

「[ネットワーク デバイス（Network Devices）] 画面からの SGA PAC の生成」（P.24-20）

SGA PAC のモニタリング

PAC プロビジョニング レポートの形式で SGA PAC プロビジョニング データを表示できます。

ステップ 1　Cisco ISE 管理ダッシュボードで、[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [セキュリティ グループ アクセス（Security Group Access）] を選択します。

ステップ 2　[PAC プロビジョニング（PAC Provisioning）] をクリックします。

ステップ 3　[時間範囲（Time Range）] ドロップダウン メニューから、レポート データを収集する時間を選択します。

ステップ 4　[実行（Run）] ボタンをクリックして指定された期間にレポートを実行します。

関連項目

第 26 章「レポート」

SGA CoA

Cisco ISE では SGA 許可変更（CoA）がサポートされています。これを使用すると、Cisco ISE でセキュリティ グループの変更を SGA デバイスに通知でき、デバイスでは関連データの取得要求でこれに応答できるようになります。

CoA 通知では、SGA ネットワーク デバイスをトリガーし、環境 CoA またはポリシーごとの CoA のいずれかを送信できます。

ここでは、次の内容について説明します。

CoA でサポートされるネットワーク デバイス

Cisco ISE は次のネットワーク デバイスに CoA 通知を送信します。

- 単一の IP アドレスを持つネットワーク デバイス（サブネットはサポートされません）
- SGA デバイスとして設定されているネットワーク デバイス
- CoA サポート対象として設定されているネットワーク デバイス

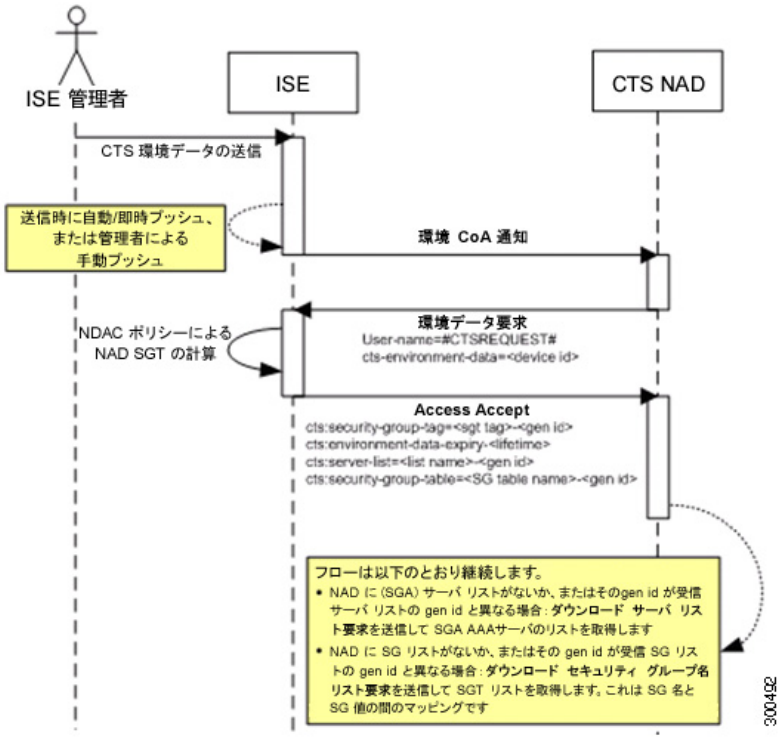
複数のセカンダリが存在する分散環境に Cisco ISE が展開されており、これらのセカンダリがそれぞれ異なるデバイス セットと相互運用している場合、CoA 要求は Cisco ISE プライマリ ノードからすべてのネットワーク デバイスに送信されます。そのため、SGA ネットワーク デバイスは、Cisco ISE プライマリ ノードで CoA クライアントとして設定されている必要があります。

デバイスは、Cisco ISE プライマリ ノードに CoA NAK または ACK を返します。ただし、SGA CoA の後に続く SGA セッションは、関連する Cisco ISE セカンダリ ノードによって処理されます。

環境 CoA

図 24-2 に、環境 CoA 通知のフローを示します。

図 24-2　　環境 CoA 通知のフロー



1. Cisco ISE は、SGA ネットワーク デバイスに環境 CoA 通知を送信します。
2. デバイスは、環境要求を返します。
3. 環境データ要求への応答で、Cisco ISE は次の情報を返します。

a. 要求を送信したデバイスの環境データ：これには、（NDAC ポリシーから推測される）SGA デバイスの SGT およびダウンロード環境 TTL が含まれます。

b. SGA AAA サーバ リストの名前および生成 ID。

c. （複数の可能性がある）SGT テーブルの名前および生成 ID：これらのテーブルには SGT 名と SGT 値がリストされ、一緒に SGT の完全リストも保持されます。

4. デバイスが SGA AAA サーバ リストを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、AAA サーバ リストの内容を取得します。

5. デバイスが応答にリストされている SGT テーブルを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、その SGT テーブルの内容を取得します。

環境 CoA の開始

環境 CoA は次のものに関して開始できます。

- 「ネットワーク デバイスに関する環境 CoA のトリガー」（P.24-23）
- 「セキュリティ グループに関する環境 CoA のトリガー」（P.24-23）
- 「SGA AAA サーバに関する環境 CoA のトリガー」（P.24-24）
- 「NDAC ポリシーに関する環境 CoA のトリガー」（P.24-24）

ネットワーク デバイスに関する環境 CoA のトリガー

ネットワーク デバイスに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　ネットワーク デバイスを追加または編集します。

ステップ 3　[SGA 属性（SGA Attributes）] セクションの下にあるセキュリティ グループ パラメータを更新します。

環境 TTL の変更は、変更が発生した特定の SGA ネットワーク デバイスにのみ通知されます。

単一のデバイスのみが影響を受けるため、環境 CoA 通知は送信直後に送信されます。結果として、そのデバイスの環境 TTL が更新されます。

セキュリティ グループに関する環境 CoA のトリガー

セキュリティ グループに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティ グループ アクセス（Security Group Access）] > [セキュリティ グループ（Security Groups）] を選択します。

ステップ 2　[セキュリティ グループ（security group）] ページで、SGT の名前を変更します。これにより、その SGT のマッピング値の名前が変更されます。これで環境変更がトリガーされます。

ステップ 3　複数の SGT の名前を変更した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての SGA ネットワーク デバイスに送信され、変更されたすべての SGT の更新が提供されます。

SGA AAA サーバに関する環境 CoA のトリガー

SGA AAA サーバに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [SGA AAA サーバ（SGA AAA Servers）] を選択します。

ステップ 2　[SGA AAA サーバ（SGA AAA Servers）] ページで、SGA AAA サーバの設定を作成、削除、または更新します。これで環境変更がトリガーされます。

ステップ 3　複数の SGA AAA サーバを設定した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての SGA ネットワーク デバイスに送信され、変更されたすべての SGA AAA サーバの更新が提供されます。

NDAC ポリシーに関する環境 CoA のトリガー

NDAC ポリシーに関する環境 CoA をトリガーするには、次の手順を実行します。

[NDAC ポリシー（NDAC policy）] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。

[NDAC ポリシー（NDAC policy）] ページで [プッシュ（Push）] ボタンをクリックすることで、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての SGA ネットワーク デバイスに送信され、「環境 CoA」（P.24-22）で説明されているとおり、ネットワーク デバイス自体の SGT の更新を提供します。

ポリシーごとの CoA

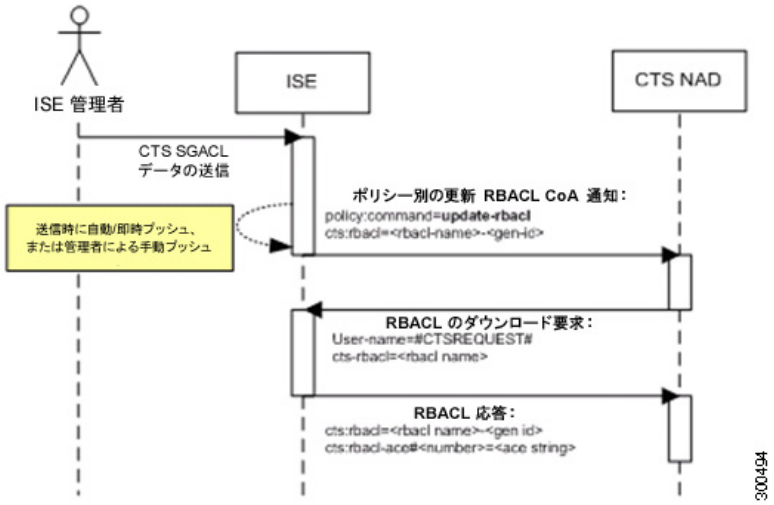
ポリシーごとの CoA 通知には 3 つのタイプがあります。

- RBACL 名前付きリストの更新 CoA：SGACL（RBACL）のダウンロード要求をトリガーします。
- SGT マトリクスの更新 CoA：特定の宛先 SGT に関連するすべての出力ポリシー セルの（出力ポリシー カラムへの）ダウンロード要求をトリガーします。
- ポリシーの更新 CoA：これは、1 つの CoA 通知で、RBACL コンテンツと出力ポリシー セルの両方に対する複数要求を開始できる、最も効果的な方法です。

RBACL 名前付きリストの更新 CoA

図 24-3 に、RBACL 名前付きリストの更新 CoA のフローを示します。

図 24-3　RBACL 名前付きリストの更新 CoA 通知のフロー



1. Cisco ISE は、SGA ネットワーク デバイスに RBACL 名前付きリストの更新 CoA 通知を送信します。通知には、SGACL 名と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGACL（RBACL）データ要求で応答できます。
   a. SGACL が、デバイスが保持する出力セルに含まれている場合。デバイスには出力ポリシー データのサブセットが保持されます。これらは、そのネイバー デバイスおよびエンドポイントの SGT に関連するセルです（選択した宛先 SGT の出力ポリシー カラム）。
   b. CoA 通知内の生成 ID が、この SGACL 用にデバイスが保持している生成 ID と異なっている。
3. SGACL データ要求への応答で、Cisco ISE は SGACL のコンテンツ（ACE）を返します。

RBACL 名前付きリストの更新 CoA の開始

RBACL 名前付きリストの更新 CoA をトリガーするには、次の手順を実行します。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] を選択します。

ステップ 2　左側の [結果（Results）] ナビゲーション ペインから、[セキュリティ グループ アクセス（Security Group Access）] の隣にある [>] ボタンをクリックし、[セキュリティ グループ ACL（Security Group ACLs）] をクリックします。

ステップ 3　「セキュリティ グループ アクセス コントロール リストの設定」（P.24-10）の説明に従って、SGACL を追加または編集します。

SGACL を送信すると、SGACL の生成 ID が変更されます。

ステップ 4　複数の SGACL のコンテンツを変更した後、[プッシュ（Push）] ボタンをクリックして、RBACL 名前付きリストの更新 CoA 通知を開始します。この通知は、すべての SGA ネットワーク デバイスに送信され、関連するデバイスのその SGACL コンテンツの更新が提供されます。

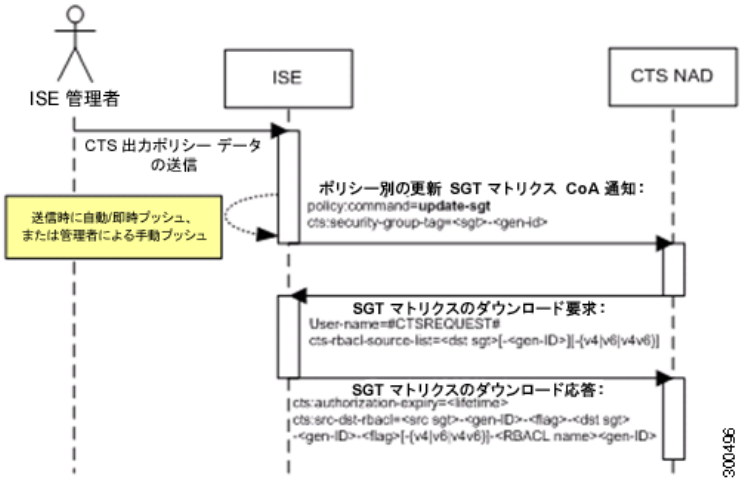
SGACL の名前または IP バージョンを変更しても、その生成 ID は変更されません。そのため、RBACL 名前付きリストの更新 CoA 通知を送信する必要はありません。

ただし、出力ポリシーで使用中の SGACL の名前または IP バージョンを変更することは、その SGACL を含むセルが変更されることを意味するため、この変更でそのセルの宛先 SGT の生成 ID が変更されます。出力ポリシーの変更について説明されている「出力ポリシーからの、SGT マトリクスの更新 CoA の開始」（P.24-26）を参照してください。

SGT マトリクスの更新 CoA

図 24-4 に、SGT マトリクスの更新 CoA のフローを示します。

図 24-4　SGT マトリクスの更新 CoA のフロー



1. Cisco ISE は、SGA ネットワーク デバイスに SGT マトリクスの更新 CoA 通知を送信します。通知には、SGT 値と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGT データ要求で応答できます。
   a. SGT がネイバー デバイスまたはエンドポイントの SGT である場合。デバイスは、ネイバー デバイスおよびエンドポイントの SGT に関連するセルをダウンロードして保持します（宛先 SGT）。
   b. CoA 通知内の生成 ID が、この SGT 用にデバイスが保持している生成 ID と異なっている。
3. SGT データ要求に対する応答で、Cisco ISE は、送信元および宛先 SGT、セルのステータス、そのセルに設定されている SGACL 名の順序リストなど、すべての出力セルのデータを返します。

出力ポリシーからの、SGT マトリクスの更新 CoA の開始

ステップ 1　[ポリシー（Policy）] > [セキュリティ グループ アクセス（Security Group Access）] > [出力ポリシー（Egress Policy）] を選択します。

ステップ 2　[出力ポリシー（Egress Policy）] ページで、セルの内容（ステータス、SGACL）を変更します。

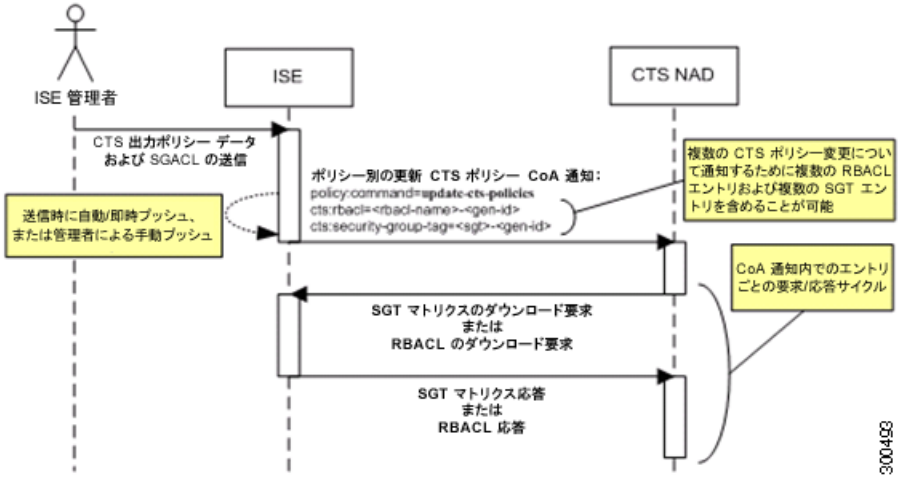
ステップ 3　変更を送信すると、そのセルの宛先 SGT の生成 ID が変更されます。

ステップ 4　複数の出力セルの内容を変更した後、[プッシュ（Push）] ボタンをクリックして、SGT マトリクスの更新 CoA 通知を開始します。この通知は、すべての SGA ネットワーク デバイスに送信され、関連するデバイスのセルの内容の更新が提供されます。

ポリシーの更新 CoA

図 24-5 に、ポリシーの更新 CoA のフローを示します。

図 24-5　ポリシーの更新 CoA のフロー



1. Cisco ISE は、SGA ネットワーク デバイスにポリシーの更新 CoA 通知を送信します。通知には、複数の SGACL 名とその生成 ID、および複数の SGT 値とその生成 ID が含まれることがあります。
2. デバイスは、複数の SGACL データ要求か複数の SGT データ、またはその両方で応答できます。
3. 各 SGACL データ要求または SGT データ要求に対する応答で、Cisco ISE は関連するデータを返します。

SGA CoA の概要

表 24-4 に、SGA CoA の開始を要求するさまざまなシナリオ、各シナリオで使用される CoA のタイプ、および関連する UI ページの概要を示します。

表 24-4　SGA CoA の概要

UI ページ	CoA をトリガーする操作	トリガー方法	CoA のタイプ	送信先
ネットワーク デバイス（Network Device）	ページの [SGA] セクションでの環境 TTL の変更	SGA ネットワークデバイスで正常に送信が行われたとき	環境	特定のネットワーク デバイス
SGA AAA サーバ（SGA AAA Server）	SGA AAA サーバの変更（作成、更新、削除、順序変更）	[SGA AAA サーバ（SGA AAA servers）] リスト ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての SGA ネットワーク デバイス
セキュリティ グループ（Security Group）	SGT の変更（作成、名前変更、削除）	[SGT] リスト ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての SGA ネットワーク デバイス
NDAC ポリシー（NDAC Policy）	NDAC ポリシーの変更（作成、更新、削除）	[NDAC ポリシー（NDAC policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての SGA ネットワーク デバイス
SGACL	SGACL ACE の変更	[SGACL] リスト ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	RBACL 名前付きリストの更新	すべての SGA ネットワーク デバイス
	SGACL 名または IP バージョンの変更	[SGACL] リスト ページの [プッシュ（Push）] ボタンまたは出力テーブルのポリシー プッシュ ボタンをクリックすると、累積された変更をプッシュできます。	SGT マトリクスの更新	すべての SGA ネットワーク デバイス
出力ポリシー（Egress Policy）	SGT の生成 ID を変更するすべての操作	[出力ポリシー（egress policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	SGT マトリクスの更新	すべての SGA ネットワーク デバイス

SGA CoA のモニタリング

SGA CoA 通知は、アラーム、ログ、およびレポートとして表示できます。

ここでは、次の表示を行う手順について説明します。

- 「SGA CoA アラーム」（P.24-29）
- 「SGA CoA レポートの実行」（P.24-29）

SGA CoA アラーム

CoA が CoA-NAK を返すとアラームが生成されます。

SGA CoA アラームを表示するには、[操作（Operations）] > [アラーム（Alarms）] > [ルール（Rules）] に移動します。

ライブ ログでも SGA CoA アラームを表示できます。ライブ ログを表示するには、[操作（Operations）] > [アラーム（Alarms）] > [受信トレイ（Inbox）] に移動します。

SGA CoA レポートの実行

次のように SGA CoA レポートを実行できます。

ステップ 1　Cisco ISE 管理ダッシュボードで、[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [セキュリティ グループ アクセス（Security Group Access）] を選択します。

ステップ 2　[実行（Run）] ドロップダウン メニューから、レポート データを収集する時間を選択します。

[実行（Run）] ボタンを使用してレポートを特定の期間だけ実行するか、[クエリーおよび実行（Query and Run）] オプションを使用できます。[クエリーおよび実行（Query and Run）] オプションを使用すると、さまざまなパラメータを使用して出力に対するクエリーを実行することができます。