アクセス制御のオブジェクト

オブジェクトとは、コンフィギュレーションで使用するための再利用可能なコンポーネントです。インライン IP アドレス、サービス、名前などの代わりに、Cisco ASA コンフィギュレーションでオブジェクトを定義し、使用できます。オブジェクトを使用すると、コンフィギュレーションのメンテナンスが容易になります。これは、一箇所でオブジェクトを変更し、このオブジェクトを参照している他のすべての場所に反映できるからです。オブジェクトを使用しなければ、1 回だけ変更するのではなく、必要に応じて各機能のパラメータを変更する必要があります。たとえば、ネットワーク オブジェクトによって IP アドレスおよびサブネット マスクが定義されており、このアドレスを変更する場合、この IP アドレスを参照する各機能ではなく、オブジェクト定義でアドレスを変更することだけが必要です。

オブジェクトのガイドライン

IPv6 のガイドライン

IPv6 のサポートには次の制約が伴います。

- 1 つのネットワーク オブジェクト グループの中で IPv4 および IPv6 のエントリを混在させることができますが、NAT に対しては、混合オブジェクト グループは使用できません。

その他のガイドラインと制限事項

- オブジェクトおよびオブジェクト グループは同じネーム スペースを共有するため、オブジェクトの名前は固有のものでなければなりません。「Engineering」という名前のネットワーク オブジェクト グループと「Engineering」という名前のサービス オブジェクト グループを作成する場合、少なくとも 1 つのオブジェクト グループ名の最後に識別子（または「タグ」）を追加して、その名前を固有のものにする必要があります。たとえば、

「Engineering_admins」と「Engineering_hosts」という名前を使用すると、オブジェクト グループの名前を固有のものにして特定可能にすることができます。

- ACL またはアクセス ルールで、送信元または宛先アドレス、あるいは送信元または宛先サービスに複数の項目を入力すると、ASDM でそれらの項目に対してプレフィックス DM_INLINE のオブジェクト グループが自動的に作成されます。これらのオブジェクトは、オブジェクト ページには表示されませんが、デバイスでは定義されています。
- オブジェクト名は、文字、数字、および .!@#$%^&()-_{} を含めて、64 文字までに制限されています。オブジェクト名は、大文字と小文字が区別されます。
- （アクセス ルールの詳細設定で）前方参照をイネーブルにしない限り、コマンドで使用されているオブジェクトを削除したり、空にすることはできません。

オブジェクトの設定

次の各項では、主にアクセス コントロールで使用されるオブジェクトを設定する方法について説明します。

ネットワーク オブジェクトとグループの設定

ネットワーク オブジェクトおよびグループは、IP アドレスまたはホスト名を特定します。これらのオブジェクトをアクセス コントロール リストで使用して、ルールを簡素化できます。

ネットワーク オブジェクトの設定

1 つのネットワーク オブジェクトには、1 つのホスト、ネットワーク IP アドレス、IP アドレスの範囲、または完全修飾ドメイン名（FQDN）を入れることができます。

また、オブジェクトに対して NAT ルールをイネーブルにすることもできます（FQDN オブジェクトを除く）。オブジェクト NAT の設定の詳細については、Network Address Translation（NAT）を参照してください。

手順

ステップ 1 [Configuration] > [Firewall] > [Objects] > [Network Objects/Group] を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] > [Network Object] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3 オブジェクトの [Type] フィールドと [IP version] フィールドに基づいて、オブジェクトのアドレスを設定します。

- [Host]：単一ホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- [Network]：ネットワーク アドレス。IPv4 の場合は、マスクを含めます。たとえば、**IP address** = 10.0.0.0 **Netmask** = 255.0.0.0。IPv6 の場合は、**IP Address** = 2001:DB8:0:CD30:: **Prefix Length** = 60 のように、プレフィックスを含めます。
- [Range]：アドレスの範囲。 IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。
- [FQDN]：完全修飾ドメイン名。つまり、www.example.com のようなホスト名。

ステップ 4 [OK] をクリックし、続いて [Apply] をクリックします。

これでルールの作成時にこのネットワーク オブジェクトを使用できます。オブジェクトを編集した場合、変更内容は自動的にそのオブジェクトを使用するすべてのルールに継承されます。

ネットワーク オブジェクト グループの設定

ネットワーク オブジェクト グループには、インライン ネットワークやホストと同様に複数のネットワーク オブジェクトを含めることができます。ネットワーク オブジェクト グループは、IPv4 と IPv6 の両方のアドレスの混在を含めることができます。

ただし、IPv4 と IPv6 が混在するオブジェクト グループや、FQDN オブジェクトが含まれているオブジェクト グループを、NAT に使用することはできません。

手順

ステップ 1 [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] > [Network Object Group] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3 次の技法を組み合わせて使用して、グループにネットワーク オブジェクトを追加します。

- **既存のネットワーク オブジェクト/グループ**：すでに定義されているネットワーク オブジェクトまたはグループを選択し、[Add] をクリックしてグループに含めます。
- **新しいネットワーク オブジェクト メンバの作成**：新しいネットワーク オブジェクトの条件を入力し、[Add] をクリックします。オブジェクトに名前を付ける場合、変更を適用すると新しいオブジェクトが作成され、グループに追加されます。ホストまたはネットワークを追加する場合、名前は任意です。

ステップ 4 すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのネットワーク オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

サービス オブジェクトとサービス グループの設定

サービス オブジェクトとグループでは、プロトコルおよびポートを指定します。これらのオブジェクトをアクセス コントロール リストで使用して、ルールを簡素化できます。

サービス オブジェクトの設定

サービス オブジェクトには、単一のプロトコル仕様を含めることができます。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Service Object/Group]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] > [Service Object] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3 サービス タイプを選択し、必要に応じて詳細を入力します。

- プロトコル：0 ～ 255 の範囲の数値または**ip**、**tcp**、**udp**、**gre** などの既知の名前。
- ICMP、ICMP6：メッセージ タイプとコードのフィールドを空白のままにすると、ICMP/ICMP バージョン 6 のあらゆるメッセージに一致させることができます。ICMP タイプを名前または番号（0 ～ 255）で指定することで、オブジェクトをそのメッセージ タイプに制限できます（オプション）。タイプを指定する場合、そのタイプ（1 ～ 255）に対する ICMP コードを任意で指定できます。コードを指定しない場合は、すべてのコードが使用されます。
- TCP、UDP、SCTP：送信元、宛先、またはその両方に対して、任意でポートを指定できます。ポートは、名前または番号で指定できます。次の演算子を含めることができます。
  - **<**：より小さい。たとえば、<80
  - **>**：より大きい。たとえば、>80
  - **!=**：等しくない。たとえば、!=80
  - **-**（ハイフン）：値の包括的な範囲。たとえば、100-200

ステップ 4 [OK]、続いて [Apply] をクリックします。

サービス グループの設定

1 つのサービス オブジェクト グループには、さまざまなプロトコルが混在しています。必要に応じて、それらを使用するプロトコルの送信元および宛先ポート、および ICMP のタイプおよびコードを入れることができます。

始める前に

ここで説明する一般的なサービス オブジェクト グループを使用して、すべてのサービスをモデル化できます。ただし、ASA 8.3(1) よりも前に使用可能であったサービス グループ オブジェクトのタイプを設定することもできます。こうした従来のオブジェクトには、TCP/UDP/TCP-UDP ポート グループ、プロトコル グループ、および ICMP グループが含まれます。これらのグループのコンテンツは、ICMP6 または ICMP コードをサポートしない ICMP グループを除く、一般的なサービス オブジェクト グループの関連する設定に相当します。これらの従来のオブジェクトを使用したい場合は、object-service コマンドに関する説明を Cisco.com のコマンド リファレンスで確認してください。

手順

ステップ 1 [Configuration] > [Firewall] > [Objects] > [Service Objects/Groups] を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] > [Service Group] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3 次の技法を組み合わせて使用して、グループにサービス オブジェクトを追加します。

- **既存のサービス/サービス グループ**：すでに定義されているサービス、サービス オブジェクト、またはグループを選択し、[Add] をクリックしてグループに含めます。
- **新しいメンバの作成**：新しいサービス オブジェクトの条件を入力し、[Add] をクリックします。オブジェクトに名前を付ける場合、変更を適用すると新しいオブジェクトが作成され、グループに追加されます。そうでない場合、名前のないオブジェクトはこのグループだけのメンバです。TCP-UDP オブジェクトに名前を付けることはできません。これらはそのグループだけのメンバです。

ステップ 4 すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのサービス オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

ローカル ユーザ グループの設定

作成したローカル ユーザ グループは、アイデンティティ ファイアウォールをサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールでも使用できるようになります。

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザ グループについて、Active Directory サーバに LDAP クエリを送信します。ASA は、そのグループをアイデンティティ ベースのルール用にインポートします。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザ グループには、Active Directory からインポートされる、ネストされたグループおよびユーザ グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。

ユーザは、ローカル ユーザ グループと Active Directory からインポートされたユーザ グループに属することができます。

ACL でユーザ名とユーザ グループ名を直接使用できるため、次の場合にだけローカル ユーザ グループを設定する必要があります。

- ローカル データベースで定義されているユーザのグループを作成する。
- AD サーバで定義されている単一のユーザ グループでキャプチャされなかったユーザまたはユーザ グループのグループを作成する。

手順

ステップ 1 [Configuration] > [Firewall] > [Objects] > [Local User Groups] を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3 次のいずれかの方法を使用して、オブジェクトにユーザまたはグループを追加します。

- **既存のユーザまたはグループを選択**：ユーザまたはグループを含むドメインを選択してから、ユーザ名またはグループ名をリストから選択し、[Add] をクリックします。リストが長い場合、ユーザの検索をサポートするために [Find] ボックスを使用します。名前は、選択されたドメインのサーバから取得されます。

- **ユーザ名を手動で入力**：ユーザ名またはグループ名を下部の編集ボックスに入力し、[Add] をクリックするだけです。この方法を使用すると、選択されたドメイン名は無視され、ドメイン名を指定していない場合はデフォルト ドメインが使用されます。ユーザの場合、フォーマットは *domain_name**username*; for groups, there is a double \\, *domain_name**group_name* です。

ステップ 4 すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのユーザ オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

セキュリティ グループ オブジェクト グループの設定

作成したセキュリティ グループ オブジェクト グループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールで使用できるようになります。

Cisco TrustSec と統合されているときは、ASA は ISE からセキュリティ グループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザ アイデンティティへのマッピングと、Cisco TrustSec タグからサーバ リソースへのマッピングを行います。セキュリティ グループ ACL のプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、ローカライズされたセキュリティ ポリシーを持つローカル セキュリティ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル セキュリティ グループには、ISE からダウンロードされた、ネストされたセキュリティ グループを含めることができます。ASA は、ローカルと中央のセキュリティ グループを統合します。

ASA 上でローカル セキュリティ グループを作成するには、ローカル セキュリティ オブジェクト グループを作成します。1 つのローカル セキュリティ オブジェクト グループに、1 つ以上のネストされたセキュリティ オブジェクト グループまたはセキュリティ ID またはセキュリティ グループ名を入れることができます。ユーザは、ASA 上に存在しない新しいセキュリティ ID またはセキュリティ グループ名を作成することもできます。

ASA 上で作成したセキュリティ オブジェクト グループは、ネットワーク リソースへのアクセスの制御に使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

ヒント ASA にとって不明なタグや名前を使用してグループを作成する場合、そのタグや名前が ISE で解決されるまで、そのグループを使用するすべてのルールが非アクティブになります。

手順

ステップ 1 [Configuration] > [Firewall] > [Objects] > [Security Group Object Groups] を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3 次のいずれかの方法を使用して、オブジェクトにセキュリティ グループを追加します。

- **既存のローカル セキュリティ グループ オブジェクト グループを選択**：すでに定義されているオブジェクトのリストから選択し、[Add] をクリックします。リストが長い場合、オブジェクトの検索をサポートするために [Find] ボックスを使用します。
- **ISE から検出されたセキュリティ グループを選択**：既存のグループのリストからグループを選択し、[Add] をクリックします。
- **セキュリティ タグまたは名前を手動で追加**：タグ番号またはセキュリティ グループ名を下部の編集ボックスに入力し、[Add] をクリックするだけです。タグは、1 から 65533 までの数字であり、IEEE 802.1X 認証、Web 認証、または ISE による MAC 認証バイパス（MAB）を通じてデバイスに割り当てられます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。有効なタグと名前については、ISE の設定を参照してください。

ステップ 4 すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのセキュリティ グループ オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

時間範囲の設定

時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能または資産に時間ベースでアクセスするために ACL ルールで使用されます。たとえば、勤務時間中にのみ特定のサーバへのアクセスを許可するアクセス ルールを作成できます。

（注） 時間範囲オブジェクトには複数の定期的エントリを含めることができます。1 つの時間範囲に absolute 値と periodic 値の両方が指定されている場合は、periodic 値は absolute の開始時刻に到達した後にのみ評価され、absolute の終了時刻に到達した後は評価されません。

時間範囲を作成してもデバイスへのアクセスは制限されません。この手順では、時間範囲だけを定義します。その後、アクセス コントロール ルールでオブジェクトを使用する必要があります。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Time Ranges]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] を選択し、新しい時間範囲を追加します。名前を入力し、任意で説明を入力します。
- 既存の時間範囲を選択し、[Edit] をクリックします。

ステップ 3 全体的な開始時刻および終了時刻を選択します。

デフォルトでは今すぐ開始し、終了することはありませんが、特定の日時を設定することもできます。時間範囲には、入力した時刻も含まれます。

ステップ 4 （オプション）時間範囲がアクティブになる曜日や週単位の繰り返し間隔など、全体的にアクティブな時間内に繰り返し期間を設定します。

a) [Add] をクリックするか、既存の期間を選択して [Edit] をクリックします。

b) 次のいずれかを実行します。

- [Specify days of the week and times on which this recurring range will be active] をクリックし、リストから日付と時刻を選択します。
- [Specify a weekly interval when this recurring range will be active] をクリックし、リストから日付と時刻を選択します。

c) [OK] をクリックします。

ステップ 5 [OK] をクリックし、さらに [Apply] をクリックします。

オブジェクトのモニタリング

ネットワーク、サービス、およびセキュリティ グループ オブジェクトに関して、個々のオブジェクトの使用状況を分析できます。[Configuration] > [Firewall] > [Objects] フォルダにある各オブジェクトのページで、[Where Used] ボタンをクリックします。

ネットワーク オブジェクトの場合、[Not Used] ボタンをクリックすると、ルールまたは他のオブジェクトで使用されていないオブジェクトを見つけることもできます。この表示によって、未使用のオブジェクトを簡単に削除できるようになります。

オブジェクトの履歴

機能名	プラットフォーム リリース	説明
オブジェクト グループ	7.0(1)	オブジェクト グループによって、ACL の作成とメンテナンスが簡素化されます。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。**class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
オブジェクト	8.3(1)	オブジェクトのサポートが導入されました。
アイデンティティ ファイアウォールでのユーザ オブジェクト グループの使用	8.4(2)	アイデンティティ ファイアウォールのためのユーザ オブジェクト グループが導入されました。
Cisco TrustSec のためのセキュリティ グループ オブジェクト グループ	8.4(2)	Cisco TrustSec のためのセキュリティ グループ オブジェクト グループが導入されました。
IPv4 および IPv6 の混合ネットワーク オブジェクト グループ	9.0(1)	以前は、ネットワーク オブジェクト グループに含まれているのは、すべて IPv4 アドレスであるか、すべて IPv6 アドレスでなければなりませんでした。現在では、ネットワーク オブジェクト グループが、IPv4 と IPv6 の両方のアドレスの混合をサポートするようになりました。 （注） 混合オブジェクト グループを NAT に使用することはできません。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Objects] > [Service Objects/Groups]、[Configuration] > [Firewall] > [Access Rule]

機能名	プラットフォーム リリース	説明
Stream Control Transmission Protocol（SCTP）のサービス オブジェクトのサポート	9.5(2)	特定の SCTP ポートに対するサービス オブジェクトおよびグループを作成できるようになりました。 **[Configuration] > [Firewall] > [Objects] > [Service Objects/Groups]** ページでサービス オブジェクトおよびグループの追加/編集ダイアログ ボックスが変更されました。