オブジェクトの設定

この章では、コンフィギュレーションで使用するための、再利用可能な名前付きオブジェクトおよびグループを設定する方法について説明します。次の項が含まれます。

オブジェクトに関する情報

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。オブジェクトは、ASA コンフィギュレーションの中で定義して、インライン IP アドレス、サービス、名前などの代わりに使用できます。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。

オブジェクトのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

- IPv6 をサポートします。
- ASA は、ネストされた IPv6 ネットワーク オブジェクト グループはサポートしません。したがって、IPv6 エントリが含まれるオブジェクトを別の IPv6 オブジェクト グループの下でグループ化することはできません。
- 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。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

- オブジェクトには、一意の名前を付ける必要があります。「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「Engnineering_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。
- オブジェクトおよびオブジェクト グループは、同じ名前スペースを共有します。
- コマンドで使用されているオブジェクトを削除したり、空にしたりすることはできません。

オブジェクトの設定

（注）　この章に記載されていない他のオブジェクトについては、次の章を参照してください。

- ローカル ユーザ：第 33 章「AAA のローカル データベースの設定」を参照してください。
- クラス マップ：ファイアウォール コンフィギュレーション ガイドの Chapter 49, “Getting Started with Application Layer Protocol Inspection,” を参照してください。
- インスペクション マップ：ファイアウォール コンフィギュレーション ガイドの Chapter 49, “Getting Started with Application Layer Protocol Inspection,” を参照してください。
- TCP マップ：ファイアウォール コンフィギュレーション ガイドの “Configuring Connection Settings” section on page 61-6 を参照してください。

ネットワーク オブジェクトとグループの設定

この項では、ネットワーク オブジェクトおよびグループの設定方法について説明します。次の項目を取り上げます。

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、または IP アドレス範囲、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）。（詳細については、ファイアウォール コンフィギュレーション ガイドの Chapter 43, “Configuring Network Object NAT (ASA 8.3 and Later),” を参照してください）。

手順の詳細

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

ステップ 2　[Add] をクリックし、[Network Object] を選択して新しいオブジェクトを追加するか、編集する既存のオブジェクトを選択して、[Edit] をクリックします。

ルール ウィンドウの [Addresses] サイド ペインで、またはルールの追加時に、ネットワーク オブジェクトを追加または編集できます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

[Add/Edit Network Object] ダイアログボックスが表示されます。

ステップ 3　次の値を入力します。

- [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は、64 文字以下である必要があります。
- [Type]：ネットワーク、ホスト、範囲、または FQDN。
- [IP Address]：ホスト アドレスまたはネットワーク アドレスの、IPv4 アドレスまたは IPv6 アドレス。このフィールドに IPv6 アドレスのコロン（:）を入力すると、[Netmask] フィールドが [Prefix Length] に変わります。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。
- [Netmask or Prefix Length]：IP アドレスが IPv4 アドレスである場合、サブネット マスクを入力します。IP アドレスが IPv6 アドレスである場合、プレフィックスを入力します。（このフィールドは、オブジェクト タイプに [Host] を入力した場合は使用できません）。
- [Description]：（任意）ネットワーク オブジェクトの説明（最大 200 文字）。

（注）　ネットワーク オブジェクトへの NAT ルールの追加の詳細については、ファイアウォール コンフィギュレーション ガイドの Chapter 43, “Configuring Network Object NAT (ASA 8.3 and Later),” を参照してください。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックして、設定を保存します

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 ネットワークと同様に複数のネットワーク オブジェクトを入れることができます。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サポートできます。

制約事項

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。

手順の詳細

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

ステップ 2　[Add] > [Network Object Group] をクリックして、新規オブジェクトまたは新規オブジェクト グループを追加します。

ルール ウィンドウの [Addresses] サイド ペインで、またはルールの追加時に、ネットワーク オブジェクト グループを追加または編集できます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

[Add Network Object Group] ダイアログボックスが表示されます。

ステップ 3　[Group Name] フィールドで、グループ名を入力します。

a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は、64 文字以下である必要があります。

ステップ 4　（任意）[Description] フィールドで、説明を長さ 200 文字以内で入力します。

ステップ 5　既存のオブジェクトまたはグループを新しいグループに追加したり（グループのネストが可能）、新しいアドレスを作成してグループに追加したりできます。

- 既存のネットワーク オブジェクトまたはグループを新しいグループに追加するには、[Existing Network Objects/Groups] ペインでオブジェクトをダブルクリックします。

  または、オブジェクトを選択して、[Add] をクリックします。オブジェクトまたはグループが右側の [Members in Group] ペインに追加されます。
- 新しいアドレスを追加するには、[Create New Network Object Member] 領域で値を入力し、[Add] をクリックします。

  オブジェクトまたはグループが右側の [Members in Group] ペインに追加されます。このアドレスはネットワーク オブジェクト リストにも追加されます。

オブジェクトを削除するには、[Members in Group] ペインでオブジェクトをダブルクリックするか、またはオブジェクトを選択して [Remove] をクリックします。

ステップ 6　すべてのメンバ オブジェクトを追加し終えたら、[OK] 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。ここでは、サービス オブジェクト、サービス グループ、TCP と UDP のポート サービス グループ、プロトコル グループ、および ICMP グループを設定する方法を説明します。説明する項目は次のとおりです。

サービス オブジェクトの設定

サービス オブジェクトは、プロトコル、ICMP、ICMPv6、TCP、または UDP のポートあるいはポート範囲を含むことができます。

手順の詳細

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

ステップ 2　ドロップダウン リストから [Add] > [Service Object] を選択します。

ステップ 3　[Name] フィールドに、サービス オブジェクトの名前を入力します。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は、64 文字以下である必要があります。

ステップ 4　[Service Type] フィールドから必要なタイプ [tcp]、[udp]、[icmp]、または [icmp6 protocol] を選択します。

ステップ 5　（任意）サービス タイプとして tcp または udp を選択した場合は、次を入力します。

- Destination Port/Range
- [Source Port/Range]：プロトコルの送信元ポート / 範囲を一覧表示します。
- [Description]：サービス グループの説明を一覧表示します。

ステップ 6　（任意）サービス タイプとして icmp または icmp6 を選択した場合は、次を入力します。

- [ICMP Type]：サービス グループの ICMP タイプを一覧表示します。
- [ICMP Code]：（任意）1 ～ 255 から選択します。
- [Description]：（任意）サービス グループの説明を一覧表示します。

ステップ 7　（任意）サービス タイプとしてプロトコルを選択した場合は、次を入力します。

- [Protocol]：サービス グループ プロトコルを一覧表示します。
- [Description]：（任意）サービス グループの説明を一覧表示します。

ステップ 8　[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、TCP または UDP の送信元および宛先のポートも入れることができます。

手順の詳細

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

ステップ 2　ドロップダウン リストから [Add] > [Service Group] を選択します。

[Add Service Group] ダイアログボックスが表示されます。

ステップ 3　[Name] フィールドに、新しいサービス グループの名前を入力します。最大 64 文字の名前を設定できます。この名前は、すべてのオブジェクト グループに対して一意である必要があります。サービス グループの名前は、他のオブジェクトやグループと同じ名前を共有できません。

ステップ 4　[Description] フィールドで、サービス グループの説明（長さ 200 文字以内）を入力します。

ステップ 5　既存のサービス オブジェクトまたはグループ、または定義済みプロトコルやポートに追加するには、[Existing Service/Service Group] オプション ボタンをクリックし、[Name] フィールドからエントリを選択し、[Add] をクリックします。

ステップ 6　新しいサービスを作成するには、[Create new member] オプション ボタンをクリックし、ドロップダウン リストからサービス タイプを選択。

- tcp、udp、または tcp/udp を選択した場合は、名前、宛先ポート / 範囲、送信元ポート / 範囲およびオプションの説明を入力します。
- icmp または icmp6 を選択した場合は、名前、ICMP タイプ（Existing Service/Service Group のリストから）、ICMP コード（0 ～ 255 の値）、およびオプションの説明を入力します。
- プロトコルを選択する場合は、名前、プロトコル、およびオプションの説明を入力します。

[Add] をクリックして、新しいサービスを追加します。

ステップ 7　[OK]、続いて [Apply] をクリックします。

TCP または UDP ポート サービス グループの設定

TCP または UDP サービス グループには、特定のプロトコル（TCP、UDP、または TCP-UDP）のポートのグループが含まれます。

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

ステップ 2　ドロップダウン リストから [Add] > [TCP Service Group]、[UDP Service Group] または [TCP-UDP Service Group] を選択します。

[Add Service Group] ダイアログボックスが表示されます。

ステップ 3　[Name] フィールドに、新しいサービス グループの名前を入力します。最大 64 文字の名前を設定できます。この名前は、すべてのオブジェクト グループに対して一意である必要があります。サービス グループの名前は、他のオブジェクトやグループと同じ名前を共有できません。

ステップ 4　[Description] フィールドで、サービス グループの説明（長さ 200 文字以内）を入力します。

ステップ 5　既存のサービス グループ、または定義済みのポートを追加するには、[Existing Service/Service Group] オプション ボタンをクリックし、[Name] フィールドからエントリを選択し、[Add] をクリックします。

ステップ 6　新しいポートを作成するには、[Create new member] オプション ボタンをクリックして、ポートの名前、番号、または範囲を入力し、[Add] をクリックして新しいポートを追加します。

ステップ 7　[OK]、続いて [Apply] をクリックします。

ICMP グループの設定

1 つの ICMP グループに、複数の ICMP タイプが含まれます。

手順の詳細

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

ステップ 2　ドロップダウン リストから [Add] > [ICMP Group] を選択します。

[Add ICMP Group] ダイアログボックスが表示されます。

ステップ 3　[Name] フィールドに、新しい IGMP グループの名前を入力します。最大 64 文字の名前を設定できます。この名前は、すべてのオブジェクト グループに対して一意である必要があります。ICMP グループ名は、他のオブジェクトおよびグループと同じ名前を共有できません。

ステップ 4　[Description] フィールドで、ICMP グループの説明（長さ 200 文字以内）を入力します。

ステップ 5　既存の ICMP グループ、または定義済みのタイプを追加するには、[Existing Service/Service Group] オプション ボタンをクリックし、[Name] フィールドからエントリを選択し、[Add] をクリックします。

ステップ 6　新しいタイプを作成するには、[Create new member] オプション ボタンをクリックして、タイプの名前または番号を入力し、[Add] をクリックして新しいタイプを追加します。

ステップ 7　[OK]、続いて [Apply] をクリックします。

プロトコル グループの設定

1 つのプロトコル グループに、複数の IP プロトコル タイプが含まれます。

手順の詳細

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

ステップ 2　ドロップダウン リストから [Add] > [Protocol Group] を選択します。

[Add Protocol Group] ダイアログボックスが表示されます。

ステップ 3　[Name] フィールドに、新しいグループの名前を入力します。最大 64 文字の名前を設定できます。この名前は、すべてのオブジェクト グループに対して一意である必要があります。グループの名前は、他のオブジェクトやグループと同じ名前を共有できません。

ステップ 4　[Description] フィールドで、グループの説明（長さ 200 文字以内）を入力します。

ステップ 5　既存のプロトコル グループ、または定義済みのプロトコルを追加するには、[Existing Service/Service Group] オプション ボタンをクリックし、[Name] フィールドからエントリを選択し、[Add] をクリックします。

ステップ 6　新しいプロトコルを作成するには、[Create new member] オプション ボタンをクリックして、プロトコルの名前または番号を入力し、[Add] をクリックして新しいプロトコルを追加します。

ステップ 7　[OK]、続いて [Apply] をクリックします。

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（IDFW）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 クエリーを送信します。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。

前提条件

IDFW をイネーブルにするには、第 38 章「アイデンティティ ファイアウォールの設定」を参照してください。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Local User Groups] ペインを開きます。

ユーザ グループとそのメンバーのテーブルが表示されます。

ステップ 2　グループを追加するには、[Add] をクリックします。[Add User Object Group] ダイアログが表示されます。

ステップ 3　グループの名前と説明を入力します。

グループ名には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。グループ名にスペースを含める場合は、名前全体を引用符で囲みます。

ステップ 4　[Domain] リストで、このグループのユーザのデフォルト ドメインを選択するか、[Manage] をクリックして新しいドメインを追加するか、既存のドメインを編集します。

ステップ 5　このグループに既存のグループを追加するには、テキスト ボックスに検索文字列を入力し、[Find] をクリックします。

ステップ 6　グループにユーザを追加するには、テキスト ボックスに検索文字列を入力し、[Find] をクリックします。

ステップ 7　グループを選択し、[Add] ボタンをクリックして、グループに追加します。

ステップ 8　ユーザを選択し、[Add] ボタンをクリックして、グループに追加します。

ステップ 9　[OK] をクリックして変更を保存します。

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 アクセス リスト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、ASA には、グローバルには定義されていない、ローカライズされたネットワーク リソースが存在することがあり、そのようなリソースにはローカル セキュリティ グループとローカライズされたセキュリティ ポリシーが必要です。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。

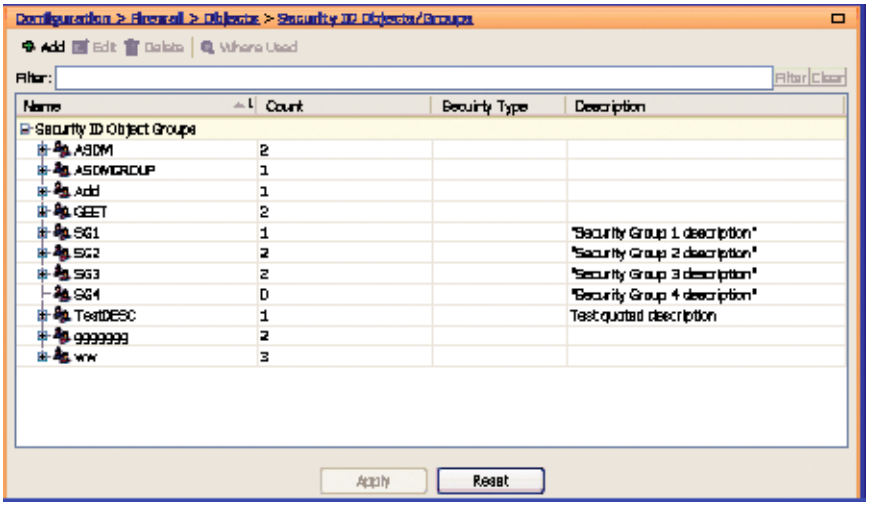
ASA 上で作成したセキュリティ オブジェクト グループは、ネットワーク リソースへのアクセスの制御に使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

前提条件

TrustSec をイネーブルにするには、第 39 章「Cisco TrustSec と統合するための ASA の設定」を参照してください。

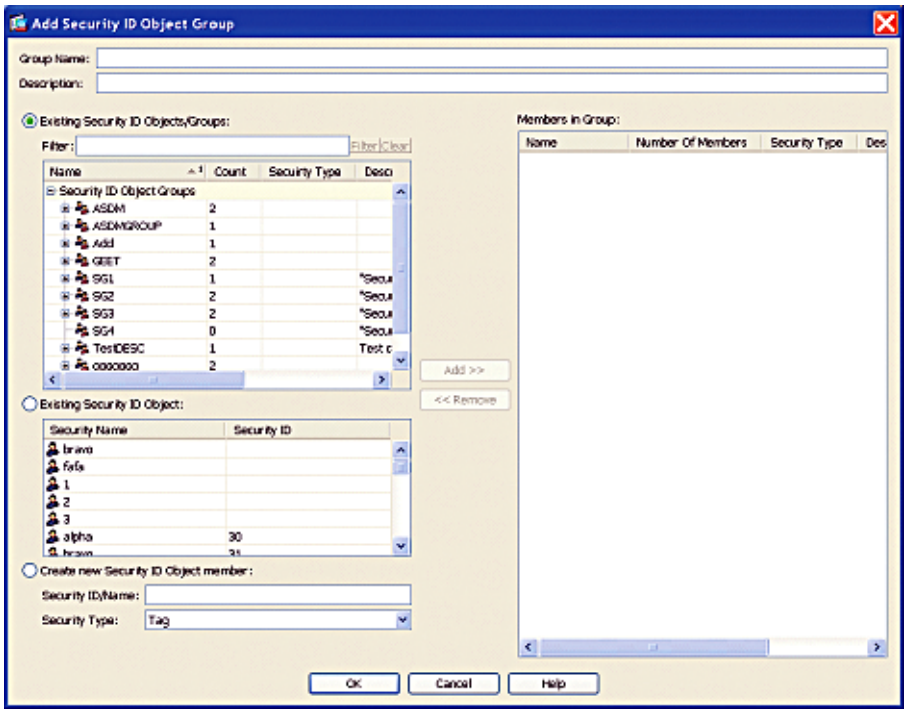
手順の詳細

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Objects] > [Security Group Object Groups] を選択します。[Security Group Object Groups] ペインが表示されます。



[Security Group Object Groups] ペインは、セキュリティ オブジェクト グループのメンバを一覧表示し、[Count] 列にのメンバ数を表示します。[Where Used] をクリックして、選択したセキュリティ グループ オブジェクトが、アクセス リストで使用されている、または別のセキュリティ グループ オブジェクトにネストされている場所を表示します。

ステップ 2　[Add] をクリックします。[Add Security ID Object Group] ダイアログボックスが表示されます。



ステップ 3　[Group Name] フィールドに、32 バイトの大文字と小文字が区別される文字列としてグループの名前を入力します。グループ名には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。

ステップ 4　[Description] フィールドには、グループの説明を入力します。

ステップ 5　次の作業を行って、セキュリティ グループ オブジェクトにメンバーを追加します。

a. 次のオプションのいずれかを選択します。

- [Existing Security ID Objects/Groups] オプション ボタン
- [Existing Security ID Object] オプション ボタン

  [Filter] フィールドで、セキュリティ オブジェクト ID 番号またはセキュリティ グループの名前を入力し、[Filter] をクリックします。セキュリティ グループの検索を広げるには、ワイルドカードを使用します。

b. [Add] をクリックして、グループのメンバーとして選択します。

セキュリティ オブジェクト グループには、少なくとも 1 人のメンバーが含まれている必要があります。

c. メンバーの選択と [Add] のクリックを継続します。既存のセキュリティ ID オブジェクト/グループと既存のセキュリティ ID オブジェクトを選択して、ネストされたセキュリティ オブジェクト グループを作成することができます。

ステップ 6　ローカルに定義されるオブジェクトを作成するには、次の手順にしたがいます。

a. [Create new Security ID Object member] オプション ボタンをクリックします。

b. [Security Type] ドロップダウン フィールドから、タグまたは名前を選択します。

SGT は、ISE による IEEE 802.1X 認証、Web 認証、または MAC 認証バイパス（MAB）を通し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。

c. [Security ID/Name] フィールドで、タグ セキュリティ タイプとして 1 から 65533 までの数値を入力するか、名前セキュリティ タイプとして 32 バイトの大文字と小文字が区別される文字列を入力します。

セキュリティ グループには、1 つの名前が割り当てられています。同じ名前は単一の SGT にしか関連付けることができません。

ステップ 7　[OK] をクリックします。[Security ID Objects/Groups] ペインが再表示されます。

ステップ 8　[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

正規表現の設定

正規表現の作成

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*metacharacters* を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して特定のアプリケーション トラフィックの内容と照合できます。たとえば、HTTP パケット内部の URL 文字列と照合できます。

ガイドライン

（注） 最適化のために、ASA では、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（//）が単一のスラッシュに圧縮されます。「http://」などの、一般的に 2 つのスラッシュが使用されるストリングでは、代わりに「http:/」を検索してください。

表 20-1 は、特殊な意味を持つメタ文字のリストです。

表 20-1　regex メタ文字

文字	説明	注釈
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp***)**	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 **（注）** Ctrl+V を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x***}** または **{***x***,}**	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc***]**	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc***]**	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。

表 20-1　regex メタ文字 （続き）

文字	説明	注釈
[*a-c*]	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
""	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** では一致を探すときに先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	Tab	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

手順の詳細

ステップ 1　[Configuration] > [Global Objects] > [Regular Expressions] を選択します。

ステップ 2　[Regular Expressions] 領域で、[Add] をクリックします。

[Add Regular Expression] ダイアログボックスが表示されます。

ステップ 3　[Name] フィールドで、式に 40 文字以内の名前をつけます。

ステップ 4　（任意）正規表現クラス マップの作成ダイアログボックスを使用するには、[Build] をクリックします。メタ文字の詳細については、表 20-1（P.20-12）を参照してください。

- [Build Snippet]：このエリアで、正規表現テキストの部分式を作成したり、メタ文字を [Regular Expression] フィールドに挿入したりできます。
- [Starts at the beginning of the line (^)]：部分式は行頭から開始し、開始場所はメタ文字のカレット（^）で示します。このオプションを使用して作成した部分式は、正規表現の先頭に挿入してください。
- [Specify Character String]：テキスト文字列を手動で入力します。
  - [Character String]：テキスト文字列を入力します。

  - [Escape Special Characters]：テキスト文字列に入力したメタ文字を文字そのものとして扱う場合、このボックスをオンにすると、メタ文字の前にエスケープ文字であるバックスラッシュ（\）が追加されます。たとえば、「example.com」と入力すると「example\.com」に変換されます。
  - [Ignore Case]：大文字と小文字を両方とも照合する場合、このチェックボックスをオンにすると、両方を照合するテキストが自動的に追加されます。たとえば、「cats」と入力すると「[cC][aA][tT][sS]」に変換されます。
- [Specify Character]：正規表現に挿入するメタ文字を指定します。
  - [Negate the character]：識別した文字を照合の対象外に指定します。
  - [Any character (.)]：すべての文字と一致させる、メタ文字のピリオド（.）を挿入します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
  - [Character set]：文字セットを挿入します。テキストをこのセットに含まれるすべての文字と照合します。次のようなセットがあります。

    [0-9A-Za-z]

    [0-9]

    [A-Z]

    [a-z]

    [aeiou]

    [\n\f\r\t]（改行、改ページ、復帰、タブを示す）

    たとえば、[0-9A-Za-z] の場合、部分式は 0 ～ 9 の数字と A ～ Z の大文字および小文字と照合します。
  - [Special character]：エスケープが必要な文字 \、?、*、+、|、.、[、(、^ を挿入します。エスケープ文字はバックスラッシュ（\）で、このオプションを選択すると自動的に入力されます。
  - [Whitespace character]：空白スペースには \n（改行）、\f（改ページ）、\r（復帰）、\t（タブ）があります。
  - [Three digit octal number]：8 進数を使用する ASCII 文字（3 桁まで）と一致します。たとえば、\040 はスペースを意味します。バックスラッシュ（\）は自動的に入力されます。
  - [Two digit hexadecimal number]：16 進数を使用する ASCII 文字（2 桁まで）と一致します。バックスラッシュ（\）は自動的に入力されます。
  - [Specified character]：任意の 1 文字を入力します。
- [Snippet Preview]：*表示専用*。正規表現に入力される部分式を示します。
- [Append Snippet]：部分式を正規表現の最後に追加します。
- [Append Snippet as Alternate]：部分式をパイプ記号（|）で区切って、正規表現の最後に追加します。区切られた表現の一方と照合します。たとえば、**dog|cat** は、dog または cat に一致します。
- [Insert Snippet at Cursor]：部分式をカーソル位置に挿入します。

[Regular Expression]：このエリアには、手動で入力して部分式で作成できる正規表現テキストが含まれます。その後、[Regular Expression] フィールドのテキストを選択して、選択部分に数量詞を適用できます。

- [Selection Occurrences]：[Regular Expression] フィールドのテキストを選択し、次のいずれかのオプションをクリックしてから [Apply to Selection] をクリックします。たとえば、正規表現「test me」の「me」を選択して [One or more times] を適用すると、この正規表現は「test (me)+」になります。

  - [Zero or one times (?)]：この記号よりも前の表現が 0 または 1 つあることを示す数量詞です。たとえば、**lo?se** は、lse または lose に一致します。
  - [One or more times (+)]：この記号よりも前の表現が少なくとも 1 つあることを示す数量詞です。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
  - [Any number of times (*)]：この記号よりも前の表現が 0、1、またはそれ以上あることを示す数量詞です。たとえば、**lo*se** は lse、lose、loose、などと一致します。
  - [At least]：少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は abxyxyz、abxyxyxyz などと一致します。
  - [Exactly]：*x* 回だけ繰り返します。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
  - [Apply to Selection]：数量詞を選択部分に適用します。
- [Test]：正規表現を適切なサンプル テキストでテストします。

ステップ 5　ビルド ツールを使用しない場合は、[Value] フィールドに 100 文字以内で正規表現を手動で入力します。表 20-1 のメタ文字を参照してください。

ステップ 6　追加する前に正規表現をテストするには、[Test] をクリックします。

[Test Regular Expression] ダイアログボックスが表示されます。

- [Regular Expression]：テストする正規表現を入力します。デフォルトでは、[Add/Edit Regular Expression] または [Build Regular Expression] ダイアログボックスで入力した正規表現が、このフィールドに入力されます。テスト中に正規表現を変更した場合、[OK] をクリックすると [Add/Edit Regular Expression] または [Build Regular Expression] ダイアログボックスにその変更内容が継承されます。[Cancel] をクリックすると、変更内容は失われます。
- [Test String]：正規表現で一致すると想定されたテキスト文字列を入力します。
- [Test]：[Text String] のテキスト文字列を [Regular Expression] の正規表現でテストします。
- [Test Result]：*表示専用*。テストの成功 / 失敗を示します。

正規表現クラス マップの作成

正規表現クラス マップで、1 つ以上の正規表現を指定します。正規表現クラス マップを使用して、特定のトラフィックの内容を照合できます。たとえば、HTTP パケット内の URL 文字列の照合が可能です。

前提条件

「正規表現の作成」（P.20-11）の説明に従って、正規表現を 1 つ以上作成します。

手順の詳細

ステップ 1　[Configuration] > [Global Objects] > [Regular Expressions] を選択します。

ステップ 2　[Regular Expression Classes] 領域で、[Add] をクリックします。

- [Name]：クラス マップの名前を 40 文字以内で入力します。「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラス マップですでに使用されている名前は再度使用できません。
- [Description]：説明を 200 文字以内で入力します。

- [Available Regular Expressions]：クラス マップに割り当てられていない正規表現を一覧表示します。
  - [Edit]：選択した正規表現を編集します。
  - [New]：新しい正規表現を作成します。
- [Add]：選択した正規表現をクラス マップに追加します。
- [Remove]：選択した正規表現をクラス マップから削除します。
- [Configured Match Conditions]：クラス マップの正規表現を照合タイプとともに示します。
  - [Match Type]：照合タイプを示します。正規表現の場合、常に基準の肯定一致タイプ（等号（=）を表示したアイコン）になります。また、インスペクション クラス マップで否定一致（赤丸を表示したアイコン）の作成もできます。クラス マップに正規表現が複数ある場合は、照合タイプ アイコンの隣にそれぞれ「OR」を表示し、「match any」クラス マップになっていることを示します。正規表現のいずれか 1 つと一致するだけで、トラフィックがクラス マップに一致します。
  - [Regular Expression]：このクラス マップに含まれている正規表現の名前を一覧表示します。

時間範囲の設定

再利用可能コンポーネントを作成して、その中で開始と終了の時間を定義しておき、さまざまなセキュリティ機能に適用することができます。時間範囲を 1 回だけ定義すれば、後は時間範囲を選択して、スケジューリングが必要なさまざまなオプションに適用できます。

時間範囲機能を使用して時間の範囲を定義し、トラフィックのルールやアクションに使用できます。たとえば、アクセス リストに時間範囲を設定すると、ASA のアクセスを制限できます。

時間範囲は、開始時間、終了時間、およびオプションの繰り返しエントリで構成されます。

ガイドライン

- 1 つの時間範囲に対して、複数の periodic エントリを指定できます。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。

手順の詳細

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

ステップ 2　[Add] をクリックします。

[Add Time Range] ウィンドウが表示されます。

ステップ 3　[Time Range Name] フィールドに、時間範囲の名前を入力します。ただし、スペースは使用できません。

ステップ 4　次のいずれかを実行して、[Start Time] と [End Time] を選択します。

a.　[Start Now] および [Never End] オプション ボタンをオンにして、デフォルト設定を許可します。

b. [Start at] および [End at] オプション ボタンをオンにし、リストから指定した開始時間および停止時間を選択することによって、特定の時間範囲を適用します。

時間範囲には、入力した時刻も含まれます。

ステップ 5　（任意）曜日を指定したり、時間範囲が繰り返してアクティブになる間隔を週単位で指定したりなど、追加の時間範囲の制限を指定するには、[Recurring Time Ranges] 領域で [Add] をクリックします。

[Add Recurring Time Range] ダイアログボックスが表示されます。

ステップ 6　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てから、[OK] をクリックします。
- [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てから、[OK] をクリックします。

ステップ 7　[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 オブジェクトまたはグループを使用しているルールを表示するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] ペインで拡大鏡の形をした [Find] アイコンをクリックします。

[Usages] ダイアログボックスが表示され、現在ネットワーク オブジェクトまたはグループを使用しているすべてのルールが一覧表示されます。このダイアログボックスには、そのオブジェクトが含まれるネットワーク オブジェクト グループもすべて一覧表示されます。

オブジェクトの機能履歴

表 20-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 20-2　オブジェクト グループの機能履歴

機能名	プラットフォーム リリース	機能情報
オブジェクト グループ	7.0(1)	オブジェクト グループにより、アクセス リストの作成とメンテナンスが簡略化されます。
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。

表 20-2　オブジェクト グループの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
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。
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。
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)	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。
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] > [Network Objects/Groups] [Configuration] > [Firewall] > [Access Rule]