



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 \(1 ページ\)](#)
- [オブジェクトの設定 \(2 ページ\)](#)
- [オブジェクトのモニタリング \(15 ページ\)](#)
- [オブジェクトの履歴 \(15 ページ\)](#)

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。

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。

ネットワーク サービス オブジェクトとネットワーク サービス オブジェクト グループの設定

ネットワーク サービス オブジェクトまたはネットワーク サービス オブジェクト グループでは、単一のアプリケーションを定義します。アプリケーションは、DNS ドメイン名（example.com など）、IP サブネット、およびオプションでプロトコルとポート（TCP/80 など）で構成できます。したがって、ネットワーク サービス オブジェクトまたはネットワーク サービス オブジェクト グループを使用することで、個別のネットワーク オブジェクトとサービス オブジェクトの内容を1つのオブジェクトに結合できます。

拡張 ACL でネットワーク サービス オブジェクト グループを作成して、ルートマップ（ポリシーベースルーティングで使用）、アクセスコントロールルール、および VPN フィルタで使用できます。ACL ではネットワーク サービス オブジェクト（グループではない）を直接使用できないことに注意してください。グループオブジェクトを使用するには、最初にオブジェクトをグループオブジェクトに追加する必要があります。

ドメイン名の仕様を使用すると、DNS スヌーピングによって、接続の開始前にユーザーの DNS 要求を通じて取得した IP アドレスが取得されます。これにより、接続の開始時に IP アドレスが使用可能になり、最初のパケットからルートマップとアクセスコントロールルールによって接続が正しく処理されます。

ネットワーク サービス オブジェクトのガイドライン

- ネットワーク サービス オブジェクトに DNS ドメイン名の仕様を含める場合は、DNS インスペクションが必要です。DNS インスペクションはデフォルトでイネーブルになっています。ネットワーク サービス オブジェクトを使用する場合は、無効にしないでください。
- DNS スヌーピングは、UDP DNS パケットでのみ実行され、TCP または HTTP DNS パケットでは実行されません。完全修飾ドメイン名オブジェクトとは異なり、アクセスリストでオブジェクトを使用しなくても、ネットワーク サービス ドメインの指定は即座にスヌープされます。
- DNS インスペクションポリシーマップで `dnscrypt` を有効にすることはできません。`dnscrypt` は、ネットワーク サービス オブジェクトで使用されるドメインの IP アドレスを取得するために必要な DNS スヌーピングと互換性がありません。ドメインの指定を含むネットワーク サービス オブジェクトは動作不能になり、関連するアクセスコントロールエントリは一致しません。
- 最大 1024 のネットワーク サービス グループを定義できます。ただし、この制限はアイデンティティファイアウォールのローカルユーザグループと共有されます。定義されたネットワーク サービス グループごとに、2 つ少ないユーザー グループを作成できます。

- ネットワーク サービス グループの内容は重複してもかまいませんが、ネットワーク サービス グループの完全な複製を作成することはできません。

信頼できる DNS サーバの構成

ネットワークサービス オブジェクトでドメイン名を設定すると、DNS 要求/応答トラフィックのスヌーピングによってDNS ドメイン名に対応するIPアドレスが収集され、その結果がキャッシュされます。すべてのDNS 要求/応答をスヌーピングできます。

スヌーピングされるレコードは、A、AAAA、およびMX です。解決された各名前には存続可能時間 (TTL) が適用され、最小値は2分、最大値は24時間です。これにより、キャッシュが古くならないように保証されます。

セキュリティ上の理由から、信頼するDNS サーバーを定義することでDNS スヌーピングの範囲を制限できます。信頼されていないDNS サーバーへのDNS トラフィックは無視され、ネットワークサービス オブジェクトのマッピングの取得に使用されません。デフォルトでは、設定および学習されたすべてのDNS サーバーが信頼されます。信頼できるリストを制限する場合のみ変更が必要になります。

始める前に

DNS スヌーピングは、デフォルトで有効になっているDNS インспекションに依存しています。DNS インспекションが無効になっていないことを確認してください。また、DNS スヌーピングは **dnscrypt** 機能と互換性がないため、DNS インспекション ポリシー マップでそのコマンドを有効にしないでください。

手順

- ステップ 1 [構成 (Configuration)] > [デバイス管理 (Device Management)] > [DNS] > [DNSクライアント (DNS Client)] の順に選択します。
- ステップ 2 [信頼されたDNSサーバー (Trusted DNS Server)] で、信頼するサーバーを決定するためのオプションを設定します。
 - (任意) 明示的に設定された信頼されたDNS サーバを追加または削除します。
 - [追加 (Add)] をクリックして新しいサーバを追加し、IP タイプ (IPv4 または IPv6) を選択し、サーバのIPアドレスを入力して、[OK] をクリックします。
 - アドレスを変更するには、サーバを選択し、[編集 (Edit)] をクリックします。
 - サーバを選択し、[削除 (Delete)] をクリックして信頼されたサーバのリストからそのサーバを削除します。
 - 次のオプションを選択または選択解除します。
 - [任意 (Any)] : すべてのDNS サーバを信頼し、すべてをスヌーピングします。このオプションはデフォルトでは無効になっています。

- [構成されたサーバ (Configured-Servers)] : DNS サーバグループで設定されたサーバを信頼するかどうか。このオプションは、デフォルトで有効です。
- [DHCPクライアント (DHCP-Client)] : DHCPクライアントとDHCPサーバ間のスヌーピングメッセージによって学習されたサーバが、信頼されたDNSサーバと見なされるかどうか。このオプションは、デフォルトで有効です。
- [DHCPプール (DHCP-Pools)] : デバイスインターフェイスで実行されているDHCPサーバを介してアドレスを取得するクライアントのDHCPプールに設定されているDNSサーバを信頼するかどうか。このオプションは、デフォルトで有効です。
- [DHCPリレー (DHCP-Relay)] : DHCPクライアントとDHCPサーバ間のスヌーピングリレーメッセージによって学習されたサーバが、信頼されたDNSサーバと見なされるかどうか。このオプションは、デフォルトで有効です。

ステップ3 [Apply] をクリックします。

ネットワーク サービス オブジェクトの設定

ネットワーク サービス オブジェクトでは、単一のアプリケーションを定義します。また、サブネット仕様やより一般的にはDNSドメイン名のいずれかによってアプリケーションの場所を定義します。必要に応じて、プロトコルとポートを含めて、アプリケーションの範囲を絞り込みます。

ネットワーク サービス オブジェクトは、ネットワーク サービス グループ オブジェクトでのみ使用できます。アクセス制御リストエントリ (ACE) でネットワーク サービス オブジェクトを直接使用することはできません。

手順

ステップ1 [構成 (Configuration)]>[ファイアウォール (Firewall)]>[オブジェクト (Objects)]>[ネットワークサービスオブジェクト/グループ (Network Services 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。

- [追加 (Add)]> [ネットワーク オブジェクト (Network Object)]の順に選択し、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 (オプション) App-ID フィールドにアプリケーションIDを追加します。

特定のアプリケーションに対してシスコが割り当てた1～4294967295の範囲の一意の番号です。このコマンドは、主に外部デバイスマネージャを使用する場合に使用します。

ステップ4 オブジェクトに1つ以上のメンバーを追加します。

- a) [新しいメンバーの作成 (Create New Member)] で次のいずれかを選択し、適切なアドレス情報を入力します。
- **domain** : 最大 253 文字の DNS 名。この名前は、完全修飾名 (www.example.com など) または部分的な名前 (example.com など) にすることができます。部分的な名前の場合、すべてのサブドメイン、つまりその名前を含むすべてのサーバー (www.example.com、www1.example.com、long.server.name.example.com など) に一致します。完全一致がある場合は、最も長い名前前で接続が照合されます。ドメイン名は複数の IP アドレスに解決できます。
 - **subnet** : ネットワークのアドレス。IPv4 サブネットの場合は、10.0.0.0 255.0.0.0 のように、ネットワークアドレスとマスクを含めます。IPv6 の場合は、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを含めます。適切なフィールドに値を入力します。
- b) [サービス タイプ (Service Type)] で次のいずれかを選択し、適切なフィールドに入力します。
- **protocol** : tcp、udp、ip など、接続で使用されるプロトコルです。オブジェクトをサービスに依存しないようにするには、単に **ip** と入力します。
 - **tcp** または **udp** : 1 ~ 65535 のポート番号か www などのニーモニックを入力します。単一のポートの場合は、ポート番号を入力するだけです。複数のポートの場合、次の演算子の後に番号を含めることができます。
 - < は、指定したポート番号より小さい任意のポートを意味します。
 - > は、指定したポート番号より大きい任意のポートを意味します。
 - **range** は、指定した 2 つのポートの間の任意のポートを意味します。最初のポート番号は、2 番目のポート番号よりも小さい番号でなければなりません。
- c) [追加 (Add)] をクリックして、ネットワーク サービスをオブジェクトに追加します。サービスを削除するには、そのサービスを選択して [削除 (Delete)] をクリックします。
- d) 必要なすべての仕様がオブジェクトに追加されるまで、このプロセスを繰り返します。

ステップ 5 [OK] をクリックします。

ネットワーク サービス オブジェクト グループの設定

ネットワーク サービス グループには、ネットワーク サービス オブジェクトと明示的なサブネットまたはドメインの指定を含めることができます。ポリシーベースルーティング、アクセスコントロール、および VPN フィルタのアクセスコントロールリストエントリ (ACE) でネットワーク サービス オブジェクトを使用できます。

ネットワーク サービス グループを使用して、同じ方法で処理する必要があるアプリケーションのカテゴリを定義します。たとえば、企業ハブへのサイト間 VPN トンネルではなく、イン

ターネットにトラフィックを送信するアプリケーションを定義する単一のグループを作成できます。

ネットワーク サービス オブジェクト グループに、明示的に、またはネットワーク サービス オブジェクトへの参照によって含めるアプリケーションの数に制限はありません。

手順

ステップ 1 [構成 (Configuration)] > [ファイアウォール (Firewall)] > [オブジェクト (Objects)] > [ネットワーク サービス オブジェクト/グループ (Network Services 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。

- [追加 (Add)] > [ネットワーク サービス グループ (Network 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、[編集 (Edit)] をクリックします。

ステップ 3 既存のサービスオブジェクトをグループに追加します。

- a) [既存のネットワーク サービス オブジェクト (Existing Network-Services Objects)] を選択します。
- b) [追加 (Add)] をクリックしてオブジェクトをグループに追加します。オブジェクトを削除するには、そのオブジェクトを選択して [削除 (Delete)] をクリックします。
- c) 必要なすべてのオブジェクトがグループに追加されるまで、このプロセスを繰り返します。

ステップ 4 グループ内で 1 人以上のメンバーを直接定義するには、次の手順を実行します。

- a) [新しいネットワーク サービス オブジェクト メンバーの作成 (Create New Network-Services Object Member)] を選択します。
- b) 次のいずれかを選択し、適切なアドレス情報を入力します。
 - **domain** : 最大 253 文字の DNS 名。この名前は、完全修飾名 (www.example.com など) または部分的な名前 (example.com など) にすることができます。部分的な名前の場合、すべてのサブドメイン、つまりその名前を含むすべてのサーバー (www.example.com、www1.example.com、long.server.name.example.com など) に一致します。完全一致がある場合は、最も長い名前が接続が照合されます。ドメイン名は複数の IP アドレスに解決できます。
 - **subnet** : ネットワークのアドレス。IPv4 サブネットの場合は、10.0.0.0/255.0.0.0 のように、ネットワークアドレスとマスクを含めます。IPv6 の場合は、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを含めます。適切なフィールドに値を入力します。
- c) [サービス タイプ (Service Type)] で次のいずれかを選択し、適切なフィールドに入力します。
 - **protocol** : tcp、udp、ip など、接続で使用されるプロトコルです。オブジェクトをサービスに依存しないようにするには、単に **ip** と入力します。

- **tcp** または **udp** : 1 ~ 65535 のポート番号か **www** などのニーモニックを入力します。単一のポートの場合は、ポート番号を入力するだけです。複数のポートの場合、次の演算子の後に番号を含めることができます。

- **<** は、指定したポート番号より小さい任意のポートを意味します。

- **>** は、指定したポート番号より大きい任意のポートを意味します。

- **range** は、指定した 2 つのポートの間の任意のポートを意味します。最初のポート番号は、2 番目のポート番号よりも小さい番号でなければなりません。

d) [追加 (Add)] をクリックして、ネットワーク サービスをグループに追加します。サービスを削除するには、そのサービスを選択して [削除 (Delete)] をクリックします。

e) 必要なすべての指定がグループに追加されるまで、このプロセスを繰り返します。

ステップ 5 [OK] をクリックします。

ローカル ユーザー グループの設定

作成したローカル ユーザー 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ー グループについて、Active Directory サーバーに 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 ユーザー 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 ユーザー 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ー 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。

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

ACL でユーザー名とユーザー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 ユーザー 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ーのグループを作成する。
- AD サーバーで定義されている単一のユーザー グループでキャプチャされなかったユーザーまたはユーザー 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ーまたはグループを追加します。

- **既存のユーザーまたはグループを選択**：ユーザーまたはグループを含むドメインを選択してから、ユーザー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、ユーザー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ーから取得されます。
- **ユーザー名を手動で入力**：ユーザー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。ユーザーの場合、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。

これでルール作成時にこのユーザー 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 タグからユーザーアイデンティティへのマッピングと、Cisco TrustSec タグからサーバー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。ユーザーは、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も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、勤務時間中のみ特定のサーバー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ー 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ー 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。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。

機能名	プラットフォーム リリース	説明
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)	<p>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。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Firewall] > [Objects] > [Service Objects/Groups]、 [Configuration] > [Firewall] > [Access Rule]</p>
Stream Control Transmission Protocol (SCTP) のサービスオブジェクトのサポート	9.5(2)	<p>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。</p> <p>[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。</p>
ネットワークサービス オブジェクトと、ポリシーベースのルーティングおよびアクセス制御におけるネットワークサービス オブジェクトの使用	9.17(1)	<p>ネットワークサービス オブジェクトを設定し、それらを拡張アクセス コントロール リストで使用して、ポリシーベースルーティング ルート マップおよびアクセス コントロール グループで使用できます。ネットワークサービス オブジェクトには、IP サブネットまたは DNS ドメイン名の仕様が含まれ、オプションでプロトコルとポートの仕様が含まれます。これらは、基本的にネットワークオブジェクトとサービスオブジェクトを結合します。この機能には、信頼できる DNS サーバーを定義して、DNS ドメイン名解決が信頼できる送信元から IP アドレスを確実に取得できるようにする機能も含まれています。</p> <p>次の画面が追加または変更されました。</p> <ul style="list-style-type: none"> • [Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に移動し、[Add/Edit] ダイアログボックスを追加します。 • [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] の順に移動し、[Add/Edit] ダイアログボックスを追加します。 • [Configuration] > [Firewall] > [Objects] > [Network Services Objects/Groups] • [Configuration] > [Device Management] > [DNS] > [DNS Client]
ネットワークサービス グループのサポート	9.19(1)	<p>最大 1024 のネットワーク サービス グループを定義できるようになりました。</p>

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。