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。

- 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、ネットワーク アドレス変換（NAT） を参照してください。

手順

ステップ 1 オブジェクト名を使用して、ネットワーク オブジェクトを作成または編集します： **object network** *object_name*

例：

```
hostname(config)# object network email-server
```

ステップ 2 次のいずれかのコマンドを使用して、オブジェクトにアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **host** {*IPv4_address*|*IPv6_address*}：単一のホストの 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。
- **subnet** {*IPv4_address IPv4_mask*|*IPv6_address/IPv6_prefix*}：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

- **range** *start_address end_address*：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** [**v4** | **v6**] *fully_qualified_domain_name*：完全修飾ドメイン名。つまり、www.example.com のようなホスト名アドレスを IPv4 に制限するには **v4**、IPv6 に制限するには **v6** を指定します。アドレス タイプを指定しない場合、IPv4 が使用されます。

例：

```
hostname(config-network-object)# host 10.2.2.2
```

ステップ 3 （任意）説明を追加します。**description** *string*

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 オブジェクト名を使用して、ネットワーク オブジェクト グループを作成または編集します。**object-group network** *group_name*

例：

```
hostname(config)# object-group network admin
```

ステップ 2 次のコマンドの 1 つまたは複数を使用して、ネットワーク オブジェクト グループにオブジェクトとアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **network-object host** {*IPv4_address* | *IPv6_address*}：単一のホストの 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-object** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*}：ネットワークまたはホストのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **network-object object** *object_name*：既存のネットワーク オブジェクトの名前。
- **group-object** *object_group_name*：既存のネットワーク オブジェクト グループの名前。

例：

```
hostname(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
hostname(config-network-object-group)# network-object 2001:db8:0:cd30::/60
hostname(config-network-object-group)# network-object host 10.1.1.1
hostname(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
hostname(config-network-object-group)# network-object object existing-object-1
hostname(config-network-object-group)# group-object existing-network-object-group
```

ステップ 3 （任意）説明を追加します。**description** *string*

例

3 人の管理者の IP アドレスを含むネットワーク グループを作成するには、次のコマンドを入力します。

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```

次のコマンドを入力して、さまざまな部門に所属する特権ユーザーのネットワーク オブジェクト グループを作成します。

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

その後、3 つすべてのグループを次のようにネストします。

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

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 オブジェクト名を使用して、サービス オブジェクトを作成または編集します。**object service** *object_name*

例：

```
hostname(config)# object service web
```

ステップ 2 次のいずれかのコマンドを使用して、オブジェクトにサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service** *protocol*：IP プロトコルの名前または番号（0 ～ 255）。**ip** を指定すると、すべてのプロトコルに適用されます。
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]：ICMP または ICMP バージョン 6 のメッセージ用。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。
- **service** {**tcp** | **udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*]：TCP、UDP、または SCTP 用。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。operator には次のいずれかを指定できます。
  - **lt**：小なり。
  - **gt**：大なり。
  - **eq**：等しい。
  - **neq**：非同値。
  - **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します（例：**range 100 200**）。

例：

```
hostname(config-service-object)# service tcp destination eq http
```

ステップ 3 （任意）説明を追加します。**description** *string*

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 オブジェクト名を使用して、サービス オブジェクト グループを作成または編集します。
object-group service *object_name*

例：

```
hostname(config)# object-group service general-services
```

ステップ 2 次のコマンドの 1 つまたは複数を使用して、サービス オブジェクト グループにオブジェクトとサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service-object** *protocol*：IPプロトコルの名前または番号（0～255）。**ip** を指定すると、すべてのプロトコルに適用されます。
- **service-object** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]：ICMP または ICMP バージョン 6 のメッセージ用。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。
- **service-object** {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*]：TCP、UDP、その両方、またはSCTP用。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。operatorには次のいずれかを指定できます。
  - **lt**：小なり。
  - **gt**：大なり。
  - **eq**：等しい。

- **neq**：非同値。
- **range**：値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します（例：**range 100 200**）。

- **service-object object** *object_name*：既存のサービス オブジェクトの名前。
- **group-object** *object_group_name*：既存のサービス オブジェクト グループの名前。

例：

```
hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
```

ステップ 3 （任意）説明を追加します。**description** *string*

例

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object tcp destination eq ftp
hostname(config-service-object-group)# service-object tcp-udp destination eq www
hostname(config-service-object-group)# service-object tcp destination eq h323
hostname(config-service-object-group)# service-object tcp destination eq https
hostname(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# object service SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# object service HTTPS
hostname(config-service-object)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
hostname(config-service-object-group)# service-object object HTTPS
```

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 オブェクトのガイドライン

- ネットワーク サービス オブェクトに 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。
- ネットワーク サービス オブジェクトまたはグループが ACL で使用されている場合、オブジェクトを削除しても、オブジェクトの内容がクリアされるだけです。オブジェクト自体は、設定で定義されたままになります。

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 インスペクションに依存しています。DNSインスペク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、DSNスヌーピングは **dnscrypt** 機能と互換性がないため、DNS インスペクション 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 **show dns trusted-source detail** コマンドを使用して、データパスにダウンロードされている現在の信頼できるサーバーを特定し、ネットワークサービス オブジェクト ドメインの解決に使用します。

デフォルトでは、DNS グループで構成するか、DHCP クライアント/サーバーまたはリレーを介して構成された DNS サーバーを信頼します。このコマンドにより、現在の設定と信頼されているサーバーが表示されます。

例：

```
ciscoasa# show dns trusted-source detail
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 10.163.47.11: management : N/A
    DNS Server Configured: 10.37.137.85: management : N/A
    DNS Server Configured: 10.37.142.73: management : N/A
Data-Path DNS Trusted Source (count 3): <ip>/<refcnt>; Trust-any disabled
  10.37.142.73/1
  10.37.137.85/1
  10.163.47.11/1
```

ステップ 2 （オプション）明示的に設定された信頼できる DNS サーバーを追加または削除します。

dns trusted-source *ip_list*

ip_list は、信頼できる DNS サーバーの IP アドレスのスペース区切りリストです。IPv4 アドレスと IPv6 アドレスを最大 12 個までリストできます。すべての DNS サーバーを含める場合は **any** を指定します。サーバーを削除するには、このコマンドの **no** 形式を使用します。

ステップ 3 （オプション）DNS サーバーグループで設定されたサーバーを信頼するかどうかを指定します。

dns trusted-source configured-servers

設定済みサーバーには、DNS グループまたはネームサーバーのコマンドで指定されたサーバーが含まれます。このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

ステップ 4 （オプション）デバイスインターフェイスで実行されている DHCP サーバー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 サーバーを信頼するかどうかを指定します。

dns trusted-source dhcp-pools

これらは **dhcpd dns** コマンドで設定されているサーバーであるため、IPv4 のみになります。このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

ステップ 5 （オプション）DHCP クライアントと DHCP サーバー間のスヌーピング リレー メッセージによって学習されたサーバーが、信頼できる DNS サーバーと見なされるかどうかを指定します。

dns trusted-source dhcp-relay

このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

ステップ 6 （オプション）DHCP クライアントと DHCP サーバー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ーが、信頼できる DNS サーバーと見なされるかどうかを指定します。

dns trusted-source dhcp-client

このオプションは、DHCP クライアントを使用して IP アドレスを取得するデバイスインターフェイスから取得した情報を使用して内部インターフェイスの DHCP サーバーを設定するように **dhcpd auto_config** コマンドを設定する場合に適用されます。このオプションは、デフォルトで有効です。このコマンドを無効にするには、コマンドの **no** 形式を使用します。

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めます。

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 オブジェクト名を使用して、ネットワーク サービス オブジェクトを作成または編集します。

object network-service *object_name* [**dynamic**]

名前は最大128文字で、スペースを含めることができます。スペースを含める場合、名前を二重引用符で囲む必要があります。**dynamic** キーワードは、オブジェクトが実行コンフィギュレーションに保存されず、**show object** 出力にのみ表示されることを意味します。**dynamic** キーワードは、主に外部デバイスマネージャーが使用するためのものです。

例：

```
ciscoasa(config)# object network-service webex
```

ステップ 2 次のいずれかのコマンドを使用して、1 つ以上のアプリケーションの場所とオプションサービスをオブジェクトに追加します。場所を削除するには、このコマンドの **no** 形式を使用します。これらのコマンドは、複数回入力できます。

- **domain** *domain_name* [*service*]：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** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*]：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

これらのコマンドのサービス仕様は同じです。一致する接続の範囲を制限する場合にのみ、サービスを指定します。デフォルトでは、解決済みの IP アドレスへのすべての接続がオブジェクトと一致します。

protocol [*operator port*]

引数の説明

- *protocol* は、tcp、udp、ip など、接続で使用されるプロトコルです。プロトコルのリストを確認するには ? を使用します。
- （TCP/UDP のみ）*operator* は次のいずれかです。
  - **eq** は、指定したポート番号と等しいポートを意味します。

- **lt** 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。
- **gt** 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。

- （TCP/UDP のみ）*port* は 1 ～ 65535 のポート番号か www などのニーモニックです。ニーモニックを確認するには ? を使用します。範囲の場合は 2 つのポートを指定する必要があります。最初のポートを 2 番目のポートよりも小さい番号にします。

ステップ 3 （オプション）シスコ定義のアプリケーション ID を追加します。

app-id *number*

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 （任意）最大 200 文字で説明を追加します。 **description** *string*

例

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

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 グループ名を使用して、ネットワーク オブジェクト グループを作成または編集します。

object-group network-service *group_name* [**dynamic**]

名前は最大128文字で、スペースを含めることができます。スペースを含める場合、名前を二重引用符で囲む必要があります。**dynamic** キーワードは、グループが実行コンフィギュレーションに保存されず、 show object-group の出力にのみ表示されることを意味します。**dynamic** キーワードは、主に外部デバイスマネージャーが使用するためのものです。

例：

```
ciscoasa(config)# object-group network-service SaaS_Applications
```

ステップ2 次のいずれかのコマンドを使用して、1 つ以上のアプリケーションの場所とオプションサービスをオブジェクトに追加します。場所を削除するには、このコマンドの**no**形式を使用します。これらのコマンドは、複数回入力できます。

- **network-service-member***object_name*：グループに含めるネットワーク サービス オブジェクトの名前。名前にスペースが含まれている場合は、その名前を二重引用符で囲みます。
- **domain** *domain_name* [*service*]：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** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*]：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

これらのコマンドのサービス仕様は同じです。一致する接続の範囲を制限する場合にのみ、サービスを指定します。デフォルトでは、解決済みのIPアドレスへのすべての接続がオブジェクトと一致します。

protocol [*operator port*]

引数の説明

- *protocol* は、tcp、udp、ip など、接続で使用されるプロトコルです。プロトコルのリストを確認するには ? を使用します。
- （TCP/UDP のみ）*operator* は次のいずれかです。
  - **eq** は、指定したポート番号と等しいポートを意味します。
  - **lt** 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。
  - **gt** 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。

- （TCP/UDP のみ）*port* は 1 ～ 65535 のポート番号か www などのニーモニックです。ニーモニックを確認するには ? を使用します。範囲の場合は 2 つのポートを指定する必要があります。最初のポートを 2 番目のポートよりも小さい番号にします。

ステップ 3 （任意）最大 200 文字で説明を追加します。 **description** *string*

例

事前に定義されたネットワーク サービス オブジェクトを使用して、一連の SaaS アプリケーションを設定します。

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

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 オブジェクト名を使用して、ユーザー オブジェクト グループを作成または編集します。**object-group user** *group_name*

例：

```
hostname(config)# object-group user admins
```

ステップ 2 次のコマンドの 1 つまたは複数を使用して、ユーザー オブジェクト グループにユーザーとグループを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **user** [*domain_NETBIOS_name*\]*username*：ユーザー名。ドメイン名またはユーザー名にスペースが含まれている場合は、ドメイン名とユーザー名を引用符で囲む必要があります。ドメイン名には、LOCAL（ローカル データベースで定義されているユーザー向け）、または **user-identity domain** *domain_NetBIOS_name* **aaa-server** *aaa_server_group_tag* コマンドで指定されている Active Directory（AD）のドメイン名を指定できます。AD ドメインに定義されているユーザーを追加する場合、*user_name* には、一意ではない可能性がある Common Name（CN）ではなく、一意の Active Directory sAMAccountName を指定する必要があります。ドメイン名を指定しない場合、デフォルト値が使用されます。デフォルト値は、LOCAL または **user-identity default-domain** コマンドで定義されている値のいずれかです。
- **user-group** [*domain_NETBIOS_name*\\]*username*：ユーザー グループ。ドメイン名またはグループ名にスペースが含まれている場合は、ドメイン名とグループ名を引用符で囲む必要があります。ドメイン名とグループ名を区切る二重の \\ に注意してください。
- **group-object** *object_group_name*：既存のユーザー オブジェクト グループの名前。

例：

```
hostname(config-user-object-group)# user EXAMPLE\admin
hostname(config-user-object-group)# user-group EXAMPLE\\managers
hostname(config-user-object-group)# group-object local-admins
```

ステップ 3 （任意）説明を追加します。**description** *string*

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　オブジェクト名を使用して、セキュリティ グループ オブジェクト グループを作成または編集します。**object-group security** *group_name*

例：

```
hostname(config)# object-group security mktg-sg
```

ステップ 2　次のコマンドの 1 つまたは複数を使用して、サービス グループ オブジェクト グループにオブジェクトを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **security-group** {**tag** *sgt_number* | **name** *sg_name*}：セキュリティ グループ タグ（SGT）または名前。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。
- **group-object** *object_group_name*：既存のセキュリティ グループ オブジェクト グループの名前。

例：

```
hostname(config-security-object-group)# security-group tag 1
hostname(config-security-object-group)# security-group name mgkt
hostname(config-security-object-group)# group-object local-sg
```

ステップ 3 （任意）説明を追加します。**description** *string*

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 時間範囲を作成します。**time-range** *name*

ステップ 2 （任意）時間範囲に開始時刻または終了時刻（または両方）を追加します。

absolute [**start** *time date*] [**end** *time date*]

開始時刻を指定しない場合、現在の時刻がデフォルトの開始時刻になります。

time は 24 時間形式（*hh*:*mm*）で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

date は *day month year* の形式で指定します（たとえば、**1 January 2014**）。

ステップ 3 （任意）繰り返しの期間を追加します。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

days-of-the-week には次の値を指定できます。最初の引数に曜日を 1 つ指定した場合にのみ、2 番目の曜日を指定できることに注意してください。

- **Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday**、または **Sunday**。最初の *days-of-the-week* 引数には、複数の曜日をスペースで区切って指定できます。
- **daily**
- **weekdays**
- **weekend**

time は 24 時間形式（*hh*:*mm*）で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

このコマンドを繰り返して、複数の繰り返し期間を設定できます。

例

次に、2006 年 1 月 1 日の午前 8 時に始まる絶対的な時間範囲の例を示します。終了時刻も終了日も指定されていないため、時間範囲は事実上無期限になります。

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

次に、平日の午前 8 時～午後 6 時に毎週繰り返される定期的な時間範囲の例を示します。

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

次の例では、時間範囲の終了日を設定し、平日の期間を午前 8 時～午後 5 時に設定し、火曜日、木曜日と比較して月曜日、水曜日、金曜日に対して午後 5 時の後に異なる時間数を加算します。

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

オブジェクトのモニタリング

オブジェクトおよびグループをモニターするには、次のコマンドを入力します。

- **show access-list**

  アクセスリストのエントリを表示します。オブジェクトを含むエントリは、オブジェクトのコンテンツに基づいて個々のエントリへも拡大しています。

- **show running-config object** [**id** *object_id*]

  現在のすべてのオブジェクトを表示します。**id** キーワードを使用すると、単一のオブジェクトを名前別に表示できます。

- **show running-config object** *object_type*

  現在のオブジェクトをタイプ、ネットワーク、またはサービス別に表示します。

- **show running-config object-group** [**id** *group_id*]

  現在のすべてのオブジェクト グループを表示します。**id** キーワードを使用すると、単一のオブジェクト グループを名前別に表示できます。

- **show running-config object-group** *grp_type*

  現在のオブジェクト グループをグループ タイプごとに表示します。

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。 **object-group** *protocol*、**object-group** *network*、**object-group** *service*、**object-group** *icmp_type* の各コマンドが導入または変更されました。
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。 次のコマンドが導入または変更されました。**object-network**、**object-service**、**object-group** ネットワーク、**object-group** サービス、**network object**、**access-list extended**、**access-list webtype**、**access-list remark**。
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。 **object-network user**、**user** のコマンドが導入されました。

機能名	プラットフォーム リリース	説明
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。 **object-network security** および **security** コマンドが導入されました。
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。 **object-group network** コマンドが変更されました。
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。 **access-list extended**、**service-object**、**service** の各コマンドが導入または変更されました。
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。 次のコマンドが変更されました。**service-object**、**service**

機能名	プラットフォーム リリース	説明
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)	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。 次のコマンドが追加または変更されました：**access-list extended**、**app-id**、**clear configure object network-service**、**clear configure object-group network-service**、**clear dns ip-cache**、**clear object**、**clear object-group**、**debug network-service**、**description**、**dns trusted-source**、**domain**、**network-service-member**、**network-service reload**、**object-group network-service**、**object network-service**、**policy-route cost**、**set adaptive-interface cost**、**show asp table classify**、**show asp table network-service**、**show dns trusted-source**、**show dns ip-cache**、**show object**、**show object-group**、**show running-config**、**subnet**
ネットワークサービス グループのサポート	9.19(1)	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。

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。